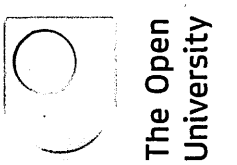
Barriers to Secure ICT in a Maritime Environment

Thesis

BARRIERS TO ICT SECURITY IN A MARITIME ENVIRONMENT



John Wood

Department of Engineering and Innovation

Faculty of Mathematics, Computing and Technology

The Open University

A thesis submitted in partial fulfilment for the degree of

Doctor of Philosophy

September 2014

DATE OF SUBMISSION: 30 NOVEMBER 2013
DATE OF AWARD: 21 OCTOBER 2014

ProQuest LLC.
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106 – 1346

Abstract

The purpose of the research reported in this thesis was to investigate the barriers to ICT security in a maritime environment so that the findings of the research can be used to develop a secure ICT maritime profile that will be capable of being updated on an on-going basis. This is an important area of research because the maritime sector is increasingly reliant upon ICT yet there is evidence that ICT security and the potential threats and consequences if ICT is not available when needed have not been given the attention they deserve. Indeed, the literature review carried out as part of this research pointed to a big gap in the maritime literature regarding ICT security.

Literature from non-maritime specific fields was used to establish a basic understanding of the barriers most likely to be relevant and provide key terminology for use in this research. Empirical data were collected from semi-structured interviews with Royal Naval personnel and informal discussions with Merchant Navy officers. A robust yet flexible approach was used to interpret the results and thus identify the barriers, many of which are caused by complex interactions between social and technical factors, particularly on-board ships.

Nine barriers to ICT security were revealed. They are: tensions experienced between security experts and ICT users; operational imperatives override security requirements; security requirements impeding business process; a limited ability to recover from disruption; unable or unwilling to share security incident information; Inadequate security training; disruption to situational awareness; unpredictable behaviour of people in difficult situations; and a lack of ICT security awareness. A new understanding of barriers arose from further interpretation of the findings, the

results of which led to recommendations for the design for an updateable maritime ICT security profile that could be used to guide relevant staff (including Ship's Security Officers) and as a tool to raise security awareness for non-experts.

Acknowledgements

I would like to thank Professor Joyce Fortune for her exceptional guidance and support throughout this remarkable period of my life. Grateful thanks go to Roger Stewart for his valued contribution during the early years of this research. I would also like to thank to Doctor Diana White who picked up from where Roger left off, and who through stimulating conversations helped me see my research in a new light on many occasions. Thanks also go to Professor Geoff Peters who provided insightful thoughts at critical moments in the development of this thesis. I would also like to thank staff of the Open University Department of Engineering and Innovation, the research school, the library and all those who have helped with the completion of this thesis. Particular thanks are due to members of the Royal Navy and Merchant Navy whose contributions have made this research possible. Final thanks are reserved for Maureen for her unwavering support and encouragement.

Declaration

Except where explicitly indicated otherwise, the ideas presented within this thesis are my own and have been generated as the result of my own original research.

List of contents

List of figures

List of tables

Acronyms, abbreviations and maritime specific terminology

AES	Advanced Encryption Standard
AIS	Automatic Identification System
ATM	Asynchronous Transfer Mode
BBC	British Broadcasting Corporation
BS7799	British Standard 7799 (Obsolete but ISO and other standards based on this BS7799)
CERT CC	Computer Emergency Response Team Co-ordination Center (Carnegie Melon Institute)
CESG	Computer Electronic Support Group (UK)
CIA	Confidentiality Integrity Availability (Also see DAD)
CIS	Communications and Information Systems (Can be the name of an organisation e.g. the CIS Division or when describing an ICT capability)
CRAMM	CCTA Risk Analysis and Management Method
C4ISTAR	Command Control Communications Computing ISTAR (MODUK)
DAD	Disclosure Alteration Destruction (The consequences of a breach in CIA)
DDoS	Distributed Denial of Service
DII	Defence Information Infrastructure (MODUK)
DoS	Denial of Service
DP	Data Protection
EMCON	Emission Control (MODUK)
ENISA	European Network and Information Security Agency
GMDSS	Global Maritime Distress and Safety System
GPS	Global Positioning System
GT	Gross Tonnage (Formerly: Gross Register Tons)
HF	High Frequency
HMG	Her Majesty's Government (United Kingdom)
HTTP	Hypertext Transfer Protocol
IA	Information Assurance
IAMM	Information Assurance Maturity Model (HMG)
ICT	Information Communications Technology
IETF	Internet Engineering Task Force
IFF	Identification Friend or Foe
IMO	International Maritime Organisation (United Nations)
INFOSEC	Information Security
IP	Internet Protocol
IPSEC	Internet Protocol Security
ISO	International Organisation for Standards
ISPS code	International Ship and Port Facility Security code
ISTAR	Intelligence, Surveillance, Target Acquisition and Reconnaissance (MODUK)
IT	Information Technology
ITSO	Information Technology Security Officer (Royal Navy)
IT system	Information Technology system
ITSy	Information Technology Security
ITU	International Telecommunications Union
JSP	Joint Service Publication (MODUK)
LAN	Local Area Network
MN	Merchant Navy (UK)
MODIS	MODUK Information Strategy
MODUK	Ministry of Defence (United Kingdom)
NATO	North Atlantic Treaty Organisation
OCTAVE	Risk assessment tool (Carnegie Melon Institute)
RFA	Royal Fleet Auxiliary (United Kingdom)
RMS	Royal Mail Ship
RN	Royal Navy (United Kingdom)

ROR	Rule of the Road for international navigation safety
RSA	Rivest, Shamirr and Adleman (Encryption algorithm)
SCADA	Supervisory Control and Data Acquisition
SKYNET 5	MODUK satellite network
SOLAS	International Convention for the Safety of Life at Sea, 1974, as amended
SSAS	Ship Security Alert System
SSA	Ship Security Assessment
SSL	Secure Socket Layer
SSO	Ship Security Officer
SSP	Ship Security Plan
SUBMISS	NATO operating procedure for incidents with submarines
SYOPS	Security Operating Procedure (MODUK)
TCP	Transmission Control Protocol
TRAM	Threat and risk analysis matrix (ISPS, IMO)
TRANSEC	Transport Security Directorate (DFT)
UDP	User Data Protocol
UK MTO	UK Maritime Trade Organisation (Royal Navy)
USB	Universal Serial Bus
VHF	Very High Frequency
VPN	Virtual Private Network
WAN	Wide Area Network
WARP	Warning Alerting Reporting Point (MODUK)
WiFi	Wireless fidelity
X1205	Cyber Security Strategy Guide (ITU)

Chapter 1

Introduction

1.1 The need for this research

The research described in this thesis stemmed from personal experience that life at sea can be fraught with difficulties. Clearly, the most obvious dangers are those associated with being in a vessel a long way from immediate assistance in an environment that is frequently hostile. These have always existed since seafaring began, but in recent years additional dangers have arisen due to a growing reliance on electronic Information and Communication Technology (ICT); specifically, the implications if ICT is not available when needed. It was my growing awareness of the very real threats posed by these dangers that led me to question what research has been done to prevent incidents involving ICT security at sea, the consequences if such an incident occurs and how to mitigate their effects. A review of the literature revealed very limited coverage of these topics which suggested an opportunity existed to undertake research to investigate barriers to ICT security in a maritime environment.

British Maritime Doctrine (Ministry of Defence UK, 2004) presents a discourse on an area referred to as 'the littoral'(p. 27) which is defined as 'a 300 mile wide multi-dimensional coastal zone in which most human activity takes place' (p. 28). This activity can have nefarious undertones as described later in Chapter 2, although more often than not, human activity at sea can be seen in a more positive light such as research, wealth generation, the opportunity to progress a career or simply recreation. In his detailed work on marine economics, Stopford (2009) points out that

the world's maritime sector can be regarded as interacting transport systems that rely increasingly on ICT. There is, however, little evidence in the maritime literature to suggest that ICT has been given adequate consideration. For example Arnaud Disaut of the National Maritime College of Ireland is credited with saying 'Marine ICT is barely studied' (Cited in Bradbury, 2013, p. 53). When maritime ICT security is considered the focus tends to be on procedural aspects. (See, for example, 'the secrecy of correspondence' (Post Office, 1975, p.2) and 'forbidding of the interception of radio communication correspondence' (Lees and Williamson, 2009, p. 153).) In its report (ENISA, 2011) of an investigation into cyber security in the European maritime sector, the European Network and Information Security Agency (ENISA) describe how the world's economy depends upon the shipping sector, and that the shipping sector in turn relies on ICT for management, operations and safety. The ENISA report emphasises the lack of research and suggests that maritime ICT security has 'essential problematic areas' (ENISA, 2011, p. 1) that are putting the availability and integrity of maritime ICT systems, and the confidentiality of the information carried on these systems, at risk. The audience for the Agency's research included 'organisations, national authorities, government bodies and private companies that are involved in the maritime sector and especially in its cyber security aspects' (p. 6). The Agency used literature regarding private/public partnerships, regulations, policies and descriptions of ICT systems together with qualitative data from interviews national authorities, government bodies and private companies and quantitate data from questionnaires 'to identify gaps and overlaps in regulations and policies, possible security issues linked to ICT systems and interesting initiatives' (p. 6). The research was validated in a workshop attended by the organisations identified in the literature. The results of their data analysis are presented in six key findings, the first

of which is 'low awareness and focus on maritime cyber security' (ENISA, 2011, p. 8). They suggest that this low level of awareness may be due to the lack of reported ICT incidents. The effect is such that there is 'a low sense-of-urgency combined with an inadequate preparedness regarding cyber risks' (p. 8). The second of their key findings is the 'complexity of the maritime ICT environment' (p. 9). They note that the ICT which supports commercial operations can be a complex mix of sophisticated technologies. (This finding complements the view of complex military ICT reported elsewhere in Chapter 1.) The Agency report cites the increasing use of Supervisory Control and Data Acquisition (SCADA) infrastructure as a specific example of the complex ICT which is increasingly used in port operations. They also note that 'there is inadequate standardisation or development of good practices to ensure that security is appropriately considered in this particular ICT environment' (ENISA, 2011, p. 9). The third of their key findings is the 'fragmented maritime governance context' (p. 11) which is leading to a lack of co-ordinated effort across the maritime sector. One contributing factor is the diverse laws and regulations which govern inland waterways, sea roads and international boundaries which makes it difficult to enforce ICT security. Another contributing factor is privatisation of national assets because 'security baselines and standards put in place may not necessarily depend on the port's country of origin, but rather on the current owner' (p. 13). The fourth of their key findings is 'the inadequate consideration of cyber security in maritime regulation' (ENISA, 2011, p. 14). Considerable effort has been applied to physical security but 'there is very little consideration given to cyber security' (p. 14). For example, the International Ship and Port Facilities Security (ISPS) Code makes no provision for the threats and vulnerabilities of cyber-attacks. The fifth of their key findings is 'no holistic approach to maritime cyber risks' (ENISA, 2011, p. 15). As a result, only a limited

range of security issues are being addressed and this is being done in an ad hoc manner. The Agency report recommends consideration of 'a holistic approach, based on sound risk management principles and good practices, in order to address the subject of maritime cyber security' (p. 15). They also suggest that the holistic security approach would require the identification of critical assets used in ports and harbours including:

- Automatic cargo handling systems
- Remote control of power and other critical services
- Ship movement management and navigation systems
- Telecommunications systems

ENISA, 2011, p. 3

The sixth of their key findings is an 'overall lack of direct economic incentives to implement good cyber security in maritime sector' (p. 16). Unlike other sectors, the maritime sector has no obvious motivation to improve their ICT security policies and practices. The Agency report suggests that it may be possible to make use of financial insurance to mitigate losses from cyber incidents including loss of data damage to networks and extortion. As a starting point, improved dialogue between insurers and the stakeholders in the maritime sector would be required. Such dialogue would potentially 'stimulate the undertaking of better cyber security measures by eliminating the barrier of the lack of awareness on cyber-risks involved' (p. 17).

The military navies of the world are responsible for keeping the sea lanes open for the 'freedom of navigation' (MODUK, 2004, p. 41). To support this, and other tasks, they rely upon complex ICT to enable the command and control of a wide range of assets ranging from ballistic missile submarines and aircraft carriers to survey vessels, tankers and off-shore patrol vessels. (See, for descriptions of maritime military

communications including voice, data, and electronic warfare, NATO (2010).) These assets are required to work in all conceivable conditions and circumstances. For example, the UK Public Accounts Committee (2013) report into Defence and cyber security notes that:

> Our Armed Forces use some of the most sophisticated equipment in the world, designed and delivered to operate in the harshest conditions that our Service Personnel find themselves in
>
> Public Accounts Committee, 2013, p. 3

Should the ICT become unavailable this reliance potentially poses a serious threat to operations and safety:

> The evidence we received leaves us concerned that with the Armed Forces now so dependent on information and communications technology, should such systems suffer a sustained cyber-attack, their ability to operate could be fatally compromised
>
> Public Accounts Committee, 2013, p. 3

The need for research is acknowledged by those in senior roles and will play a key role in the efforts to make the Ministry of Defence cyber strategy work:

> The rapidly changing nature of the cyber threat demands that a premium be placed on research and development to enable the MODUK to keep pace with, understand and anticipate that threat
>
> Public Accounts Committee, 2013, p. 9

Prior to their 2013 report, the Public Accounts Committee (2008) censured the Ministry of Defence for having 'an undesirable record on data security when it should be amongst the best in government' (p. 7). They based their criticism on incidents such as the virus which caused severe disruption to the Royal Navy's 'NavyStar' network and the loss of personnel data from unencrypted laptops. The Department estimates that, between 1 April 2004 and 31 March 2008, 747 of its laptops and 121 memory sticks have gone missing or been stolen. Since the start of this financial year, a further seven breaches have occurred, which together amount to the loss of the

personal details of at least 1.7 million people' (Public Accounts Committee, 2008, p. 21). Even elementary mistakes can lead to serious consequences. For example, a French soldier, using an unauthorised electronic memory device, accidentally loaded malicious software onto a military system which rapidly spread throughout their military network. This in turn led to the headline 'French Navy surrenders to Conficker' (The National Business Review, 2009).

1.2 Maritime ICT: Key innovations 1860 to 2013

Essentially, maritime ICT is made up of the three components in Figure 1.1. Mariners can be thought of as early adopters of ICT with over one hundred years of operating experience. Although not exclusively so, this operating experience draws on innovations in fields ranging from submarine cable technology and wireless telegraphy through to broadband Internet services and the automation of on-board systems. This section will look at these innovations in turn. This historical perspective is included so that the context of this research can be better appreciated by those not familiar with the maritime environment.

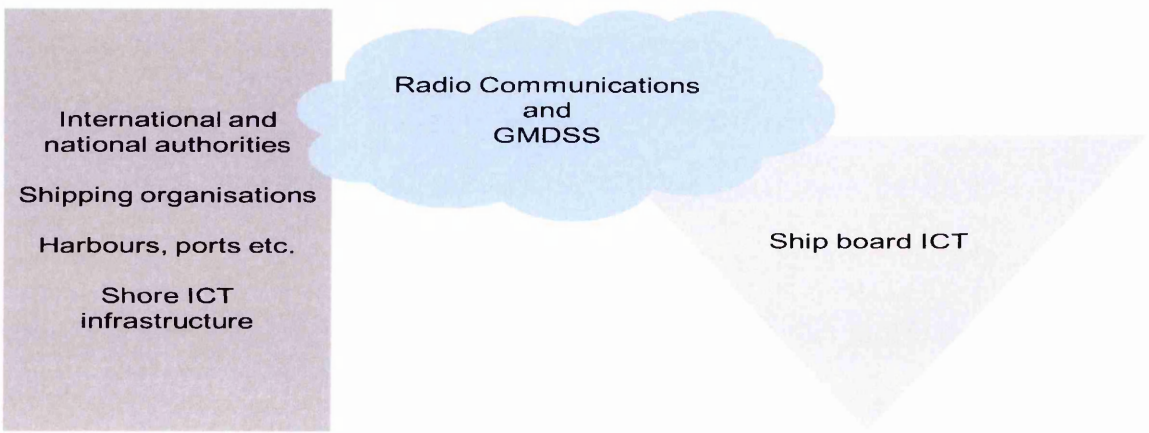


Figure 1.1: Three basic components of maritime ICT which enable the information flow needed to conduct world-wide maritime activity

From submarine cables to VPNs

Submarine cable networks effectively 'transformed the shipping business' (Stopford, 2009, p.27) when they were introduced in the 1860s. Ship arrivals and departures could be tracked in near real time which in turn allowed ship owners to bid for new cargoes with a certain confidence that had not previously existed. By the 1980s, the introduction of desk top computers and office automation tools led to the rise of private networks that use secure leased telephone lines to connect distributed offices with a degree of security. (For a description of a Private Branch Exchange see Stallings (2007).) More recently, and as noted by Roumboutsos et al. (2005), shipping companies have tended to migrate their private networks to shared virtual private networks (VPNs), over which they pass sensitive information to remote locations.

One example of the advanced technology that is used in this way is Defence Information Infrastructure (DII) (Public Accounts Committee, 2008). The DII project has replaced a number of single service systems with common to all terminal equipment, secure on-site wiring all inter-connected via a VPN. DII is also extending to front line forces such that headquarters, RN ships, army and RAF units can exchange information and command and control orders for joint operations. However, as Hill (2000) notes, VPN architectures tend to be based on the Internet Protocol with all the inherent threats and vulnerabilities they bring. For example, the timely and cost effective management of cargoes remains a core principle of an efficient merchant fleet. From a security perspective, if the associated management information could be intercepted, changed or interrupted, then a competitor could gain an advantage, such as 'the divulgation of cargo information' (ENISA, 2011, p. 15) or take advantage of the situation to smuggle contraband items (Bateman, 2013).

Operations: from wireless telegraphy to Internet protocol

Schiller (2003) notes that 'shipping was a major early client for wireless telegraphy'(p. 9) in the early 1900s and 'wireless was standard for shipping by the time the Titanic issued its radio distress calls in 1912' (p. 9). Wireless telegraphy opened up new shipping routes by allowing vessels to move off the well-worn trade routes and so exploit new regions for commerce. The introduction of wireless telephony in the 1930s and radio telex in the 1940s established the core radio capabilities available to mariners at sea today. (For examples of these core capabilities see Lees and Williamson (2009).) The combined voice and data capability of wireless radio is now referred to as radio-communication and includes 'any transmission, emission or reception of signs, signals, writings, images and sounds or intelligence of any nature by radio, optical or other electromagnetic system' (International Telecommunications Union Radio Regulations, 2008, Volume 1, p. 7). For quite some time after the introduction of wireless telegraphy, the technologies available to establish permanent links between ship and shore did not exist and so from a maritime ICT security perspective, a ship at sea had been considered to be, in effect, isolated from the threats and vulnerabilities that were acknowledge in relation to terrestrial ICT. This situation has obviously changed with the introduction of broadband real time links provided over satellite channels. One example of the advanced technology that is now used is Skynet 5. This is a military communications system provided by the commercial consortium Astrium on behalf of MODUK through a Public Private Finance Initiative (Close, 2013). For an annual fee, Astrium guarantees bandwidth availability to MODUK, whilst the contract also permits Astrium to sell spare bandwidth to NATO, allied nations and other organisations. This provision was used

to provide support to the policing effort during the 2012 London Olympics (Records from BBC News Archive, 2012). The satellites have on-board computers to support overload planning in the form of automatic routing and messaging precedence, and an advanced 'anti-jam' capability. Skynet 5 became operational in 2008 and uses Internet Protocol and the broadband technology Asynchronous Transfer Mode (ATM).

Distress: from Morse Code to GMDSS

Although the first wireless telegraphy equipment was not originally adopted to improve safety, the ability to call for help from sea was soon recognised as a major benefit. RMS Republic demonstrated the effective use of wireless radio when she foundered off the east coast of America on the 6th January 1909 after a collision with a smaller vessel, SS Florida (Watson, 1995). Even though the distress signal from the Republic was weak, it was received ashore and relayed quickly to vessels in the vicinity of the incident. The consequent rapid and co-ordinated incident response played a major part in the saving of 1,600 lives. Wireless communications also helped to save lives when RMS Titanic sank on the 15th April 1912 but in this instance the disaster also served to highlight significant communications weaknesses in the arrangements and mechanisms that were in place at the time (Mersey, 1912). Chief amongst these were shortfalls in internationally agreed distress frequencies, poor radio discipline, the lack of agreed message handling priorities and non-standard wireless watch keeping hours. As a consequence, the Radio Regulations were overhauled to include international distress, urgency, and safety protocols, radio silence periods and standard international manual radio watch keeping hours. Wireless distress, urgency and safety communications continued to rely upon a manual radio watch keeping system ashore and afloat and specially trained Morse

Code operators until 1988 when the Global Maritime Distress and Safety System (GMDSS) was introduced (Lees and Williamson, 2009). GMDSS automated the international safety radio watch keeping system and changed the way that radio operators and maintenance staff are trained and employed at sea (International Maritime Organisation, 2009). Dunston (2010) argues that GMDSS is predominately used by relatively wealthy nations and is too expensive for use by the nations of the developing world. He goes on to state that 'GMDSS implementation by many Flag States is less than satisfactory - some ships, particularly those registered under 'Flags of Convenience', are operating under exemptions, in direct breach of the Safety of Life at Sea (SOLAS) Convention'. (The SOLAS Convention was ratified by member nations as a result of the Titanic incident (Mersey, 1912).) However, Lees and Williamson (2009) suggest that GMDSS was a much needed improvement in wireless communications capability because it uses 'both terrestrial and satellite communications' (p. 1) such that if one fails there should, in principle, be alternative means of calling for help. Using satellite communications, which notionally gives global radiocommunications coverage, provides another benefit. A vessel's radio communications outfit is now determined by the Sea Area of Operation rather than the displacement of the vessel. However, as already stated, not all vessels are GMDSS compliant. The owners and crew of those that are not are required to comply with the pre GMDSS radio regulations. (See Lees and Williamson (2009) for a description of pre GMDSS requirements.)

Military vessels are exempt from Safety of Life at Sea (SOLAS) regulations and the International Naval Safety Association (2011) argues that the principle reason for these exemptions is due to the differences in safety ethos between naval and

merchant vessels. For example, the Master of a ship is legally bound to render help during an incident but in so doing they must not stand their ship into danger (IMO, 2009). The Commanding Officers of warships will also render assistance if the military circumstances allow and will, if necessary, put their ship in harms' way to save lives (International Naval Safety Association, 2011). Also, compared to a merchant vessel, a warship will almost certainly have more crew members, who are trained in disaster support and systems failure recovery methods. However, the International Naval Safety Association publication ANEP77 (NATO, 2011) does set out the safety standards required for a naval vessel to conform to merchant navy standards. It is interesting to note that as of 2013, ANEP 77 does not have an ICT security chapter but it does have a chapter on Global Maritime Distress and Safety System equivalence (Lloyd's Register, 2013).

Ship's automated systems and ICT

The automation of on-board systems enables larger displacement vessels to be built and manned with relatively fewer crew when compared to their sail powered predecessors (Stopford, 2009). The forerunners of today's ICT-enabled systems included electric telegraphs, remote steering and damage control systems. Modern merchant vessels still rely on these systems but now use common local area networks and an array of other ICT ranging from the remote control of engines and cargo monitoring to office automation. As well as for dedicated ICT, ships also make use of private ICT such as mobile telephones, laptops and other devices. This ICT poses substantial security issues caused by authorised and non-authorised equipment. For example, such equipment can interfere with ship's operations, give away a ship's position by direction finding or location tracking or allow eavesdropping

to take place. (See Section 2.2 for detailed consideration of these topics.) Examples of ship-board ICT are supplied at Figure 1.2. (For more examples of current maritime ICT capability see Digital Ship website available at www.thedigitalship.com.)

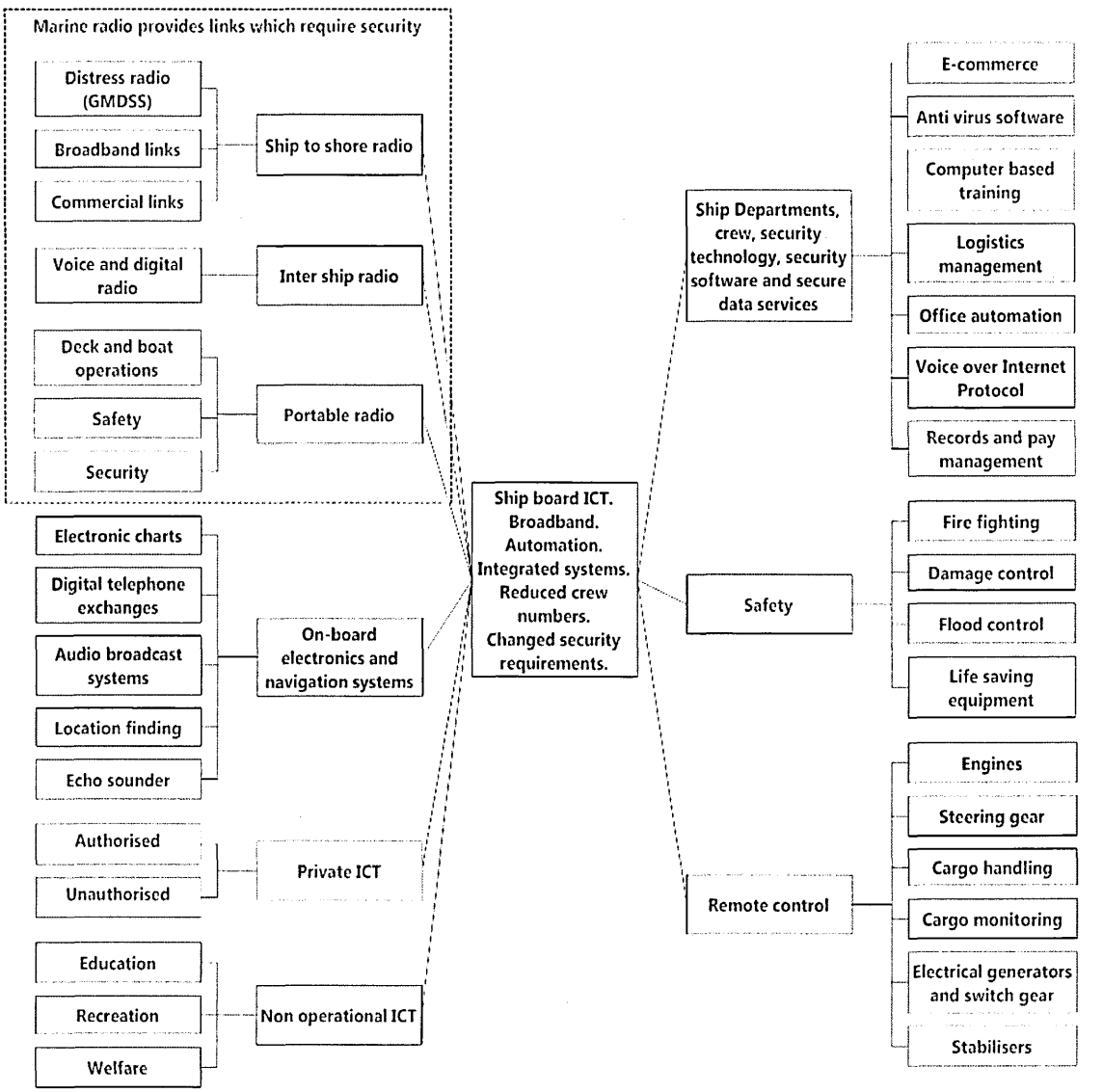


Figure 1.2: Examples of ship-board ICT drawn from multiple sources

Situating the dangers

The literature, so far, suggests that maritime systems and the way they interact is complex. It is difficult however to assess the dangers posed to these systems by an incident involving secure ICT in a maritime environment because of the apparent lack of specific literature on the subject. The Royal Navy's 'capability based approach' (Ministry of Defence, 2004, p. 172) describes the means and ability needed to achieve maritime operational objectives, whilst the associated 'Fighting Instructions' (Ministry of Defence, 2004, p. 214) sets the precedence for recovery from incidents, making use of the axiom *float move fight*. For this thesis: *float* describes the means of restoring critical ICT services; *move*, describes the ability to restore day to day ICT services throughout the ship; and *fight* is used to encapsulate all the reasons for using ICT at sea, such as trade, exploiting natural resources, war-fighting etc. Should the crew of a ship be unable to maintain the imperatives of *float move fight*, then the ability to call for help will be needed. Examples of threats to VPN security are provided as Table 1.1, and examples of threats to ICT security are listed in Table 1.2.

Table 1.1: Virtual Private Network architectures: examples of threats to security

Source	Examples of threats to security
Anderson and Moore (2009)	Virtualisation has increased the number and types of ICT that must be protected. Too easy to create virtual machines. Unknown network connections & account privileges persist. Unknown applications – whether malicious or loaded inadvertently by employees, for the latter patches are never applied. Oversights in configuration settings. Laptops are offline when vulnerability scans occur/its agent software is not activated. People not advised that vulnerability scans are to occur. Data governance is poor. People copy and move information without permissions.
Harris and Hunt (1999)	Password sniffing. Denial of Service (DoS). Session hijacking. IP spoofing. Common protocol vulnerabilities.
Kropp (2006)	Business needs brought on by deregulation. Movement towards common operating systems.
Witten and Frank (2005)	Unauthorised data mining.
Zwicky *et al.*(2000)	Re-routing. Denial of Service (DoS) and Distributed Denial of Service (DDoS). Re-tunnelling. Common gateway interface scripts. Rapid changes to technology with unknown impact on IP security functions.

Table 1.2: Examples of threats to ICT security	
Source	Examples of threats to ICT security
International Organization for Standardisation (2008)	Computer assisted fraud. Espionage. Sabotage. Vandalism. Fire. Flood.
Pillai and Andley (2010)	Governments cannot control the internet in their country. Cyber-crime. Theft of ICT assets. Electronic eavesdropping. Lack of trained investigators.
Internet Engineering Task Force (2007)	Human error. Deliberate trespass. Software attacks. Technical failures in hardware and software. Technical obsolescence.

1.3 Research aim and thesis structure

The aim of the research presented in this thesis is to advance understanding of security issues associated with the use of ICT systems in a maritime environment. Specifically, it seeks to reveal barriers to secure ICT and use them to inform the development of a secure ICT maritime profile that will be capable of being updated on an on-going basis.

Chapter 1 established the need for this research and mapped key innovations from 1860 to 2013 in order to better appreciate the context of this research. Chapter 2 reports the results of a literature review of wireless ICT, cyber security and barriers to ICT security drawn largely from non-maritime specific fields that is used to inform this research. Chapter 3 sets out the methodology and analysis used to conduct the research. Chapter 4 presents a summary and analysis of data collected from Royal Navy personnel before presenting a discussion regarding barriers and how they manifest themselves. Chapter 5 presents a summary of data collected from Merchant Navy personnel and presents information from secondary literature that allows the

consequences of a secure ICT incident to be better appreciated. Chapter 6 starts with a discussion of how the barriers that have emerged from the research can act as a stimulus to develop a secure ICT profile before using them to develop a profile that will be capable of being updated on an on-going basis. Finally, Chapter 7 summarises the research and sets out conclusions, the contribution made to knowledge and recommendations for further research. The research roadmap is shown in Figure 1.3.

Figure 1.3: Research roadmap

Chapter 2

Literature review

2.1 Introduction

The purpose of this literature review is to investigate further the background to this research into barriers to ICT security in a maritime environment. This chapter will first review wireless ICT security and the small amount of sector specific literature that has been published. It will then look at the literature on barriers with particular emphasis on issues that appear to have greater relevance to the maritime sector. At the end of the chapter, the findings from Chapters 1 and 2 will be combined to identify the key concepts that are most likely to be associated with barriers to ICT security in the maritime domain and thus potentially will help to frame the empirical research.

2.2 Wireless radio: security issues

Use of wireless systems ashore has only become widespread in recent years. Wireless devices, applications and services now enable remote access to the Internet allowing users to vote, bank, shop and interact with social networks from any location that has suitable radio coverage (Davis, 2010). This mobility has given wireless users greater flexibility in the running of their business and day to day lives and has introduced the concept of 'Mobile Web 2.0' (Davis, 2010, p. 2). When it comes to security, the mobility and flexibility of wireless systems comes with negative consequences and many authors have looked at the problems associated with wireless. For example, Dunlop and Smith (1994) note that the fundamental physical limitations of using radio frequencies are 'the spectrum available for mobile communications is limited' (p. 513) and that 'the radio environment is subject to

propagation difficulties and interference' (p. 514). Goldsmith (2005) suggests that the difficulties with propagation can lead to quality of service issues because 'the need to use the higher end of the frequency spectrum tends to induce path losses [attenuation] which limit service ranges' and that 'interference can make the channel or medium unpredictable'(pp. 6-8). The behaviour of wireless users has to be accounted for in the design of a network. For example, network topology changes as users join and leave the network which in turn can impact on the time it takes to access the required services (Rackley, 2007). Not only is the available spectrum limited but, as Goldsmith (2005) points out 'there is also heavy competition for a scarce resource [spectrum] which has to be allocated to disparate applications and systems' (pp. 11-12). The radio part of the electromagnetic spectrum is divided into frequency bands and use of each band is determined by the propagation characteristics of that band. For example, the high frequency band of 3 to 30 MHz is allocated to a variety of purposes ranging from worldwide communications to commercial radio. (For radio spectrum allocation see Clark (1997, p. 161).) The allocation and permission to use the electromagnetic spectrum for wireless applications[1] is strictly regulated and policed at both national and international levels. This allocation process can be very expensive (see, for example, the UK allocation of 3G licences (OFCOM, 2007)) and service providers have to make a return on their investment (Rackley, 2007). Interfacing with the networks of other service providers, both nationally and internationally, can also be expensive and any unnecessary overhead in the data stream will reduce the revenue earning potential of the system. (See, for example, Udupa's (1999, pp.273-274) discussion of overhead produced by cryptography algorithms.)

[1] Wireless applications include telephony, 'smart phones', Web browsers etc.

As Gratton (2007) observes 'wireless technology is used where a fixed infrastructure [wired[2]] would normally be difficult to deploy' (p. 5). For example, electricity, water and gas distribution networks are remotely controlled and monitored using Supervisory Control and Data Acquisition (SCADA) infrastructure. (See, for examples, Patel *et al.* (2009) and Piggin (2010).) The range of potential targets from shipping to manufacturing and airports makes SCADA 'an attractive target' (Piggin, 2010, p. 36). The ENISA (2011) report highlights their concern about the increased use of SCADA infrastructure in the maritime sector and the potential for 'the deliberate disruption of critical automation systems' (p. 1) by threats such as Stuxnet. Stuxnet exploits combinations of 'Zero Day' vulnerabilities, rootkit alterations and antivirus evasion and 'is one of the most complex threats they [Symantec] have analysed' (Piggin, 2010, p. 36).

Wireless radio traffic is especially at threat from eavesdropping, location tracking, deception (spoofing), jamming (denial of service) and tunnelling when compared to the wired alternatives (Zeadally *et al.*, 2007). Each of these will now be considered in turn. Stallings (2007) explains the five layers of the Internet Protocol 'peer-to-peer' architecture. These are: physical; network access; internet; host-to-host or transport; and application. As well as each layer representing a logical connection between peers, the layers also represent the point of access for attacking a network. For example, the physical layer 'specifies the characteristics of the transmission medium, the nature of the signals, the data rate and related matters' (p. 35). The transmission medium for wireless is the 'ether'[3] and the signal can be readily intercepted by anyone with suitable equipment. This leads to, perhaps, the most obvious

[2] In this context, wired refers to the fixed landlines that connect exchanges etc.
[3] The Oxford Reference Dictionary defines ether as 'a medium through which electromagnetic waves were formerly thought to be transmitted' (Oxford English, 1996, p. 481).

vulnerability of radio traffic, eavesdropping. This can come in two forms, physical and virtual, and is normally undertaken to gain an advantage. For example, Gaitskell (1998) points out that eavesdroppers are looking for passwords, address books, company data, or indeed anything that can offer a business or operational advantage and unlike other forms of attack, the eavesdropper does not want the sender or recipient of the transmission to know it has been intercepted. Virtual eavesdropping can harvest vast amounts of data very quickly. However, eavesdropping vulnerabilities are not confined to wireless radio and vital information can be exposed in conversation. As Clark (1997) points out, 'it is easier to overhear a conversation rather than hack into a network' (p. 713). Therefore, if people openly discuss sensitive security issues, and such conversations are overheard, then the eavesdroppers' job is made easy. Mann (2008) argues that there are two reasons why organisations are less than willing to acknowledge this lack of security awareness amongst employees. First, the organisations which supply hardware, software and outsourced services cannot account for the actions of employees over whom they have little control. Secondly, it is far easier to implement technical countermeasures which are tangible and as a result relatively easy to monitor and change.

Mobile wireless security is also at threat from location tracking and location finding (Lees and Williamson, 2009). Mobile telephony uses a system of 'polling' to keep track of users who are accessing the network (Rishi, 2005). A 'base station' broadcasts its location and in return the wireless device transmits a signal allowing the system to route voice and data traffic to the appropriate area. Even without specific position data, any radio device can be located by direction finding equipment. (For examples of the use of direction finding equipment see 'Station X' (Smith, 1998).)

Another position-related vulnerability of concern is 'Geo-tagging' whereby social media can be used to establish movement patterns and reveal the locations of users without the need for wireless interception (Luo *et al.*, 2011). Traffic flow analysis methods can be used to monitor data streams and radio activity to reveal patterns of use (NATO, 2010). Traffic flow security uses methods which 'conceal the presence of valid messages on wireless radio by causing the channel to appear busy at all times' (NATO, 2010, p. 165).

'Spoofing' (NATO, 2010, p. 149) can be used on a radio circuit to cause confusion and deception. Spoofing techniques include re-broadcast of edited voice messages to misdirect operations. For example, it is possible to use readily available software to record voice messages and rapidly edit and retransmit the fake message in an attempt to misdirect the legitimate listeners. A version of spoofing, known as 'phishing' (Anderson and Moore, 2009) utilises computers and telephones to direct people onto fake web sites with the aim of 'obtaining bank details and other items of private information' (p. 2717). A variant of this form attack is known as 'spear phishing' in which fraudsters will attempt to defraud using Trojans and other malicious software. (For definitions of malicious software see Pfleeger (1997, p. 179).) Jamming can be thought of as a 'Denial of Service'. As with a wired network, a jamming attack can be launched against a radio network in the form of direct flooding of the entire band, selective frequency jamming or combinations of the two. Jamming was used extensively during 1939 to 1945 in all theatres of war including the maritime environment to disrupt communications and cause confusion. The Global Positioning System (GPS) may be particularly vulnerable to jamming, as suggested by research cited in Richards (2013) 'a low power GPS jammer could stop all GPS receivers from

working correctly within a 20 mile area' (Kindle Location 1907). (For further examples of jamming see Schneier (2000) and Smith (1998).) Today, maritime military and merchant organisations are looking to Software Defined Radio and Cognitive Radio with Dynamic Spectrum Management and Dynamic Frequency Allocation in an attempt to 'make more efficient use of the electromagnetic spectrum' (Rackley, 2007, p. 343). During their analysis of the security issues arising from this technology, Leon *et al.* (2010) identified jamming as a serious threat which could deny the use of the allocated spectrum to primary and secondary spectrum users. If deployed to sea, the new technology will face the Denial of Service (DoS) threats which from malicious code that can circumvent security measures (For examples of multi-vector malicious software see Pidgeon (2010).)

The rapid changes to technology often have an unknown impact on Internet Protocol security functions (Zwicky *et al.*, 2000). For example, tunnelling is a technique which allows IP packets to cross co-operating networks. From a commercial point of view, tunnelling has the benefit of enabling telecommunications between the distributed parts of an organisation without the need to rent dedicated radio and line links which can be expensive (Hill, 2000). However, there are tunnelling techniques which can be exploited to bypass security enforcing functions. For example, wireless access networks can be vulnerable to a tunnelling form of attack, an example of which is given by Kalsson (2011). Although wireless radio continues to evolve and the benefits of flexibility and mobility are important to day to day life, it remains the case that launching an information bearing electromagnetic wave into the ether is not the best way of keeping that information private!

2.3 ICT security taxonomy

This section looks at the taxonomy of ICT security so that the security aspects of this research can be better appreciated by those not familiar with such topics. There has been a transition from the traditional fortress security paradigm of 'need to know' towards an open Internet Protocol (IP) paradigm 'need to share' in which shared infrastructures cross international boundaries. 'Need to know' is primarily concerned with protecting the confidentiality of information as described by Krutz and Vines (2003a) and is still of importance when protecting sensitive information. In an attempt to achieve a balance between need to know and need to share, security standards such as BS7799[4] were introduced. Such standards use security risk management that balance the business need to share information against the security requirements to protect information (Qingxiong and Pearson, 2005). This transition has been driven by the ubiquitous nature of ICT and Caralli (2004) has mapped the shift from 'need to know' to 'need to share' as a series of changes. The starting point was ad hoc security, in which security requirements were added as an after-thought. Next came, vulnerability-based, where vulnerabilities were accounted for at a given point in time. Then, risk-based, which uses a balance between risk, vulnerability and cost to achieve a sustainable security solution. The final stage identified by Caralli (2004) is enterprise-based, which combines risk-based security management with the needs of the business. By 2013, 'Cloud Computing' has added a new dimension to ICT security. This will be considered towards the end of this section. (For a detailed description of Cloud Computing security see Krutz and Vines (2010).)

[4] BS7799 has now been withdrawn. However, the basic principles are still valid and reflected in both the ISO 17779 standards and ISO 27000 controls.

The role of security risk management is to draw together all aspects of security in a cohesive and cost effective manner (International Organization for Standardisation, 2008). Security risk management methodologies call for a prominent management role in security (Dutta and McCrohan, 2002). To achieve ISO 27000 accreditation an organisations security management team have to demonstrate their understanding of the organisation, what the organisation is trying to achieve, where the organisation is operating and the technology they use (International Organisation for Standardisation, 2008). In his self-styled 'tongue in cheek' review of management security, Berghel (2008) discusses 'the false sense of security that can be engendered by following out of date and often obtuse standards' (p.13). Several authors (see, for example, Pfleeger (1997), Rees and Allen (2008), Kim, *et al.* (2005), Noe, *et al.* (2006), McGee, *et al.* (2007) and Herath and Herath (2008)) acknowledge the need for risk management principles to be applied early and throughout the life cycle of a project. A number of security risk assessment methods can be found in the literature. For example, the CCTA Risk Analysis and Management Method (CRAMM) is one of the UK government's ICT security risk methodologies (HMG, 2007). The CRAMM tool is also used internationally to justify the need for ICT security and to demonstrate compliance with ICT security standards. CRAMM provides a standardised method of the analysis and management of technical (hardware and software) and non-technical (physical and human) aspects of security. In order to assess these components, CRAMM is divided into two parts: Analysis which details what steps an organisation should take to identify its assets and the vulnerabilities of those assets to attack; and Management which is concerned with how to design, implement and monitor the security plan. The components of CRAMM are shown in Figure 2.1.

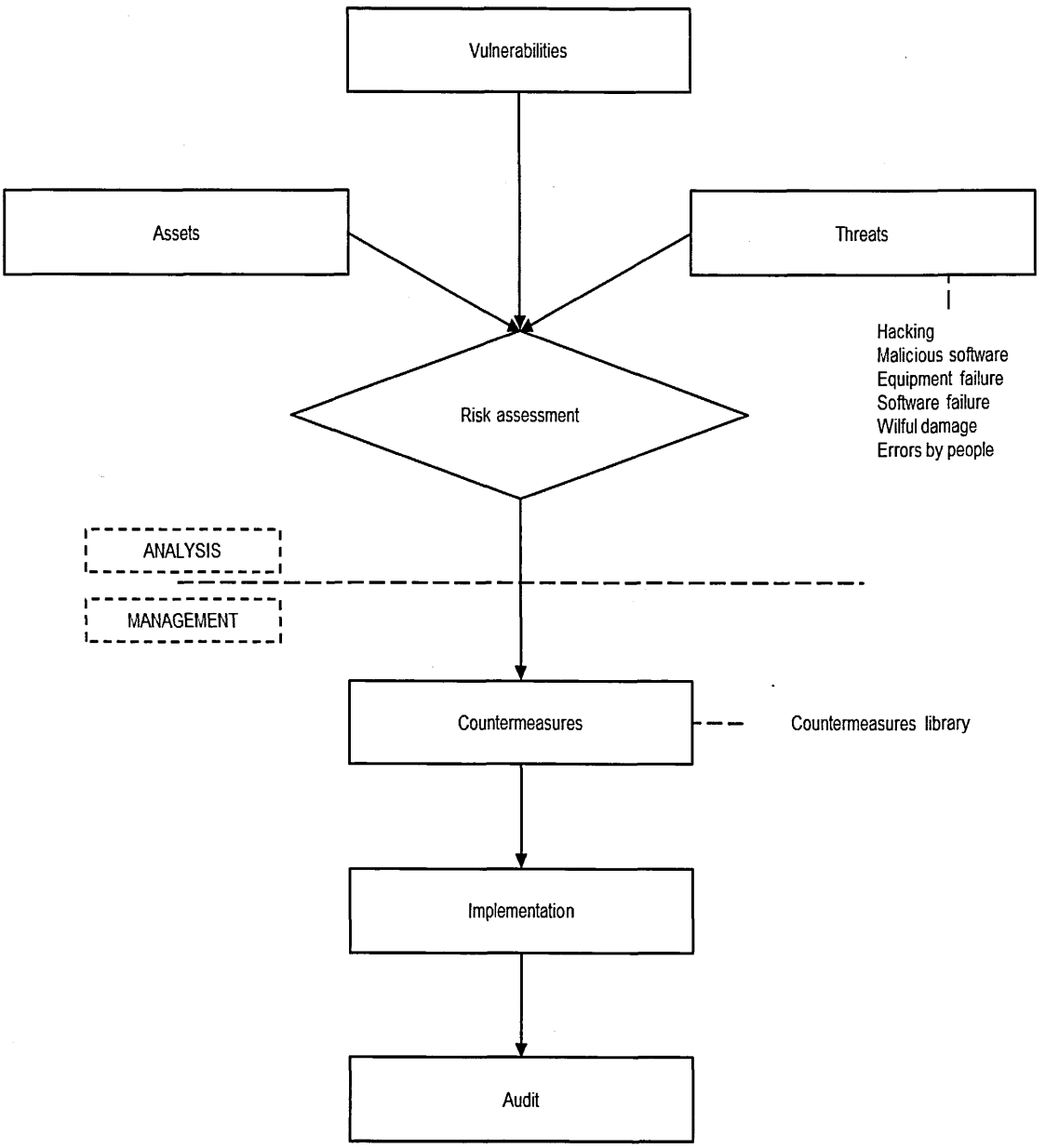


Figure 2.1: CRAMM – the components of security analysis and management (Siemens, 2007, web page)

Another security risk method is the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) (Alberts and Dorofee, 2003). (See Figure 2.2.) The OCTAVE method is based on a risk management framework and involves identifying the critical assets which require security controls. This is achieved by using an 'asset based threat profile' (Alberts and Dorofee, 2003, p. 13-14) which identifies security vulnerabilities throughout the organisation and delivery partners, and develops an organisational security strategy. When using OCTAVE, Caralli and Young (2008) suggests that there is a need to identify purposeful activity throughout an organisation, not just security activity, so that a broader enterprise wide approach to security can be taken. He argues that this wider approach is needed to take account of the complexity of ICT systems and because of the move from private leased lines and tangible assets to intangible information-based assets based on

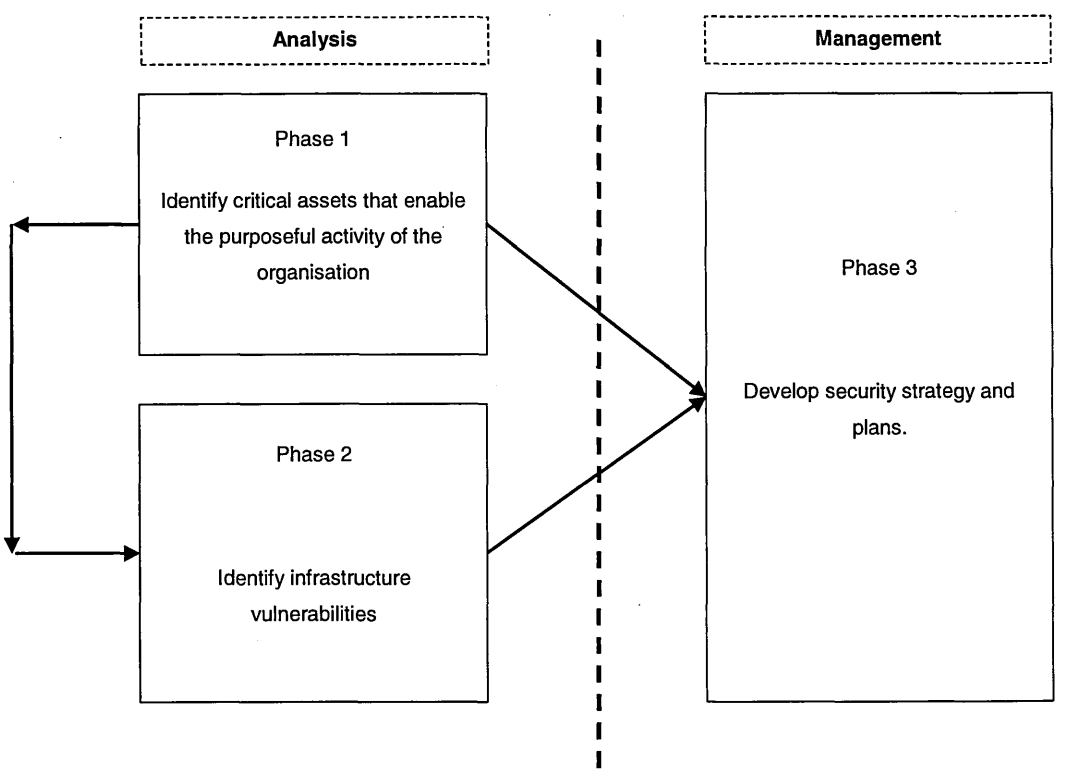


Figure 2.2: OCTAVE (Alberts and Doroffe, 2003, p.34)

'cloud' type architecture. He also points out that interconnection and interdependencies between organizations have increased dramatically and the boundaries are no longer clear. One example of an organisation that exemplifies the changes discussed by Caralli and Young (2008) is Nissan UK (Nissan, 2012) which offers an example of a modern manufacturing organisation based on outsourcing, integrated supply chains, and other external partnerships which have changed organisational boundaries and complicated the requirements of ICT security. This transition from closed bespoke architecture to open Internet Protocol architecture can lead to particular vulnerabilities to cyber-attack because cyberspace is 'seamless and goes beyond national boundaries at the speed of light' (Clarke and Knake, 2010, p. 2). Whitman and Mattord (2007) define a cyber-attack as 'an intentional or unintentional attempt to cause damage or otherwise compromise information or the systems that supports it' (p. 521). For example, re-routing where a router is forced to re-route packets because it believes there is a more efficient path. In reality, the re-routed packets are either going to a malicious address or are being used as part of a distributed denial of service attack. The International Telecommunications Union (ITU) Cyber Security Strategy Guide (International Telecommunications Union, 2011), also known as X.1205, has content that although not explicitly about barriers, does suggest objective barriers that could complicate or prevent progress towards a secure state in the maritime sector. For example:

- International legal measures do not allow crime committed across borders to be successfully prosecuted
- Technical and procedural measures cannot prevent, detect or respond to cyber attacks
- Organisational structures inadequate to prevent, detect or respond to cyber attacks
- Inadequate knowledge and expertise of cyber security
- International co-operation, dialogue and co-ordination cannot be achieved

International Telecommunications Union, 2011, pp. 20-21

The Internet Engineering Task Force publishes statistics for the categories of cyber-attack. (Statistics are available at: http://www.IETF.org.) Their categories include 'human error' which is often stated as a major cause of loss of information. For example, an administrator can create an incorrect filter setting in a firewall which in turn has the potential to compromise the system by permitting non-authorised access to sensitive areas of the system. Next, 'deliberate trespass' can be achieved using known vulnerabilities to software programs such as back-doors and bugs in the programme script. 'Theft', in a cyber-context, refers to a breach in confidentiality. The information on a system can be of high value in terms of industrial process, production costs, personnel records and other items, and their disclosure can have adverse consequences. 'Technical failures' are not as common as once they were. The reliability of computers and associated peripheral and telecommunication equipment improves with each new generation of equipment. However, the possibility of hardware and software failure still has to be accounted for in a security plan. 'Common gateway interface scripts' can be subverted at the software level in the same way as a re-routing attack. 'Technical obsolescence' is a problem when support for the system becomes more expensive and potentially vulnerable as new cyber-attack techniques overcome older defences. The Internet Engineering Task Force also classifies malicious security activity under various headings. First 'Administrative or user privileges were attempted'. For example, an attacker may attempt to subvert the system by using known or guessed access codes or passwords. Next 'a denial of service was attempted'. This is where an attacker floods a network with requests for information. This can be at the machine level (Ping attack) or at the user level (spam attack). In these cases, valuable bandwidth and processing time is denied to the user. Then there is 'an action that impacts the integrity of a file or database was attempted'.

In these cases, the attacker is attempting to change the file content to cause operating difficulties. For example, it may be possible for an attacker to change the delivery times of customer orders causing confusion and dissatisfaction. Another activity is 'an attempt to exfiltrate information'. This activity can range from key board logging to capture information such as passwords or bank details to mining for specific information which may be of some value to the attacker. Next, opportunities can be taken to 'attempt to exploit a miss-configuration in a system'. As with the earlier firewall example, any system misconfiguration can be exploited. For example, if a router can be re-programmed to transmit or receive data on an inappropriate communications channel. A popular malicious activity is 'violating a site policy'. Here, web pages can be defaced or deleted, again causing confusion and dissatisfaction. Often malicious activity involves some form of cyber reconnaissance and can be coupled with a social-engineering. The desired result is to gain any information about the system including configuration, contents and passwords. The IETF talk about 'unknown activity'. This is a useful 'catch all' for malicious activity which has yet to be recognised as such. For example, intrusion detection software may detect unexpected activity but cannot decided whether it malicious or just exceptional. Also, a 'zero day' attack maybe detected but not yet classified as malicious. Finally, 'natural causes' such as a flood or lightning strike are not the same as cyber-attacks but they can have the same or similar adverse consequences.

The notion of layered defence is a relatively common one. (Discussions of the relative merits of using layered defence to make it difficult for an attacker to succeed can be found in Pfleeger (1997, pp. 13-14), International Organisation for Standardization (2008) and Piggin (2010, p. 38).) Although the layered defence paradigm is popular it

is not always efficient in terms of providing effective ICT security because it can lead to complacency, errors in configuration and ultimately systems failure (Piggin, 2010). However, it is generally accepted that protecting against cyber-attack requires balanced layers and security management, concepts, policies and tools. (See, for example, The Open University (2008a).) There are numerous security countermeasure tools of which the following are fundamental and well reported: cryptography; firewalls; identification and authentication; antivirus software and security training. Each of these countermeasures will be examined in turn in this section.

Schneier (1996) originally argued that cryptography alone can solve security needs but later retracted this claim and instead argued that although cryptography provides an effective tool meaningful security 'involves people: things people know, relationships between people, people and how they relate to machines' (Schneier, 2000, p. xi). One of the disadvantages of using any cryptography algorithm is the simple fact that it will increase the length of the associated data stream and so will both take longer to transmit and cost more (Udupa, 1999). Even so, cryptography is still one of the principle wireless security countermeasures. The two main cryptography formats are symmetric and asymmetric (CESG, 2008a) as given in Figure 2.3. Symmetric cryptography methods are widely used by military organisations. This traditional form of cryptography is expensive because of the need for bespoke hardware and software, and the need to ensure all trusted parties have the current cryptography keys (van der Lubbe, 1998, p.131). A relatively recent development of symmetric cryptography allows the current cryptography keys to be

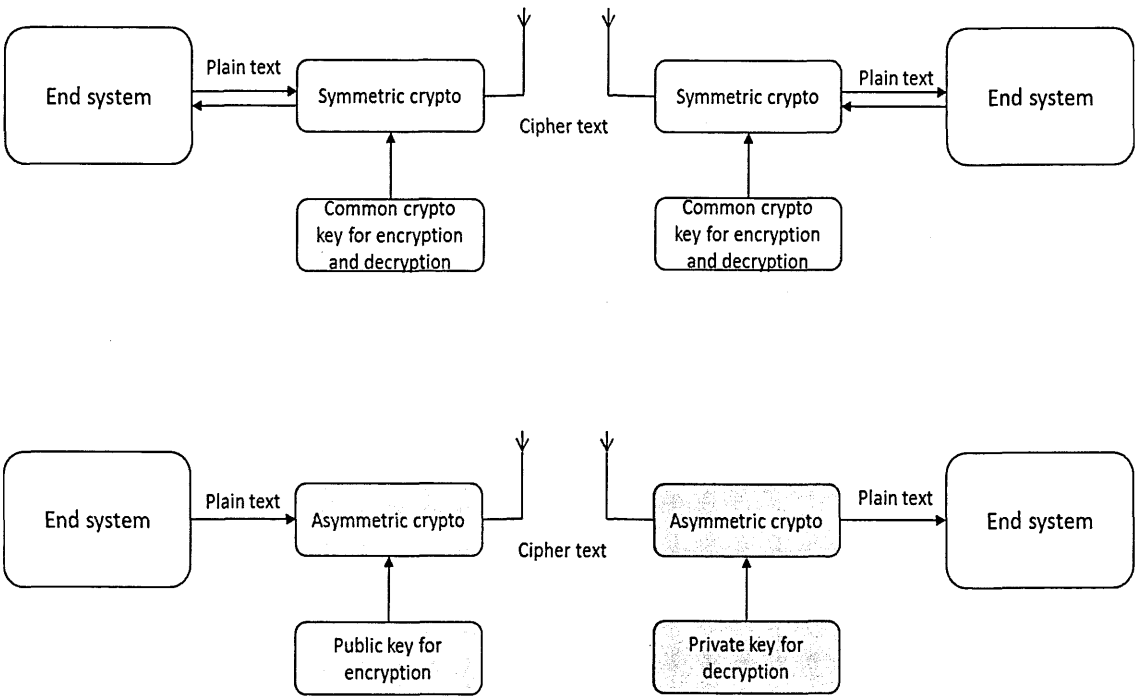


Figure 2.3 Comparison of symmetric and asymmetric cryptography

distributed over electronic media so reducing the need for a trusted physical distribution network. The Advanced Encryption Standard (AES) is an example of commercially available symmetric cryptography algorithm (The Open University, 2008b). Asymmetric cryptography works by having a private and public cryptography key which means that there is no need for expensive distribution networks. Rather, the public key can either be either sent in plain text via e-mail or stored on a trusted server which acts as a telephone directory of public keys. This works because information encrypted with a public key can only be decrypted with the equivalent private key, which must be closely guarded if security is to be maintained. It should be noted that information encrypted with the private key can be decrypted with the equivalent public key. RSA (named for Rivest, Shamir and Adleman) is an example of a commercially available asymmetric cryptography algorithm (The Open University, 2008b). Secure Socket Layers (SSL) uses a combination of both methods of

cryptography to make best use of their individual strengths and weaknesses (The Open University, 2008b). For example, symmetric encryption and decryption is faster, but needs key distribution. Asymmetric encryption and decryption is slower by comparison, but offers longer key lengths and so is potentially more secure.

Symmetric and asymmetric cryptographic methods are vulnerable to cryptanalysis. If a data stream is encrypted then cryptanalysis techniques can be used by the ill-disposed (van der Lubbe, 1998). Technically, the longer the cryptography key length then the stronger the stronger the protection (CESG, 2008a). However, keys can be stolen or lost making it possible for a third party to pose as a trusted party. Pfleeger lists three functions of a cryptanalyst:

1. Attempt to break a single message
2. Attempt to recognise patterns in encrypted messages
3. Attempt to find general weaknesses in an encryption algorithm

Pfleeger, 2000, p. 23

Another way of protecting data is to disguise its existence and this is known as Steganography; one method of which is to 'subtly merge message bits within a data stream' (Schneier, 1996, p. 1). This method is also useful for delivering virus payloads.

A firewall is intended to provide a break between the outside world and the ICT system it is designed to protect. Khalil *et al.* (2010) claim that: 'the three primary goals of network security which are confidentiality, integrity and availability can be achieved by using firewalls' (p. 204). Indeed, Zwicky points out that: 'for many people a firewall is the first and last line of defence' (p. 21). However, Zwicky also notes the limitations of firewalls in delivering network security including:

- Not a protection against an insider attack
- Using virus protection as part of the gateway process is slow

- Configuring and updating firewall software can be time consuming
- Packet flooding can occur and so leave the internal network vulnerable

Zwicky, 2000, p. 24

The purpose of identification and authentication is to stop unauthorised access and represents one of the original countermeasures developed for ICT security. Traditional identification and authentication requires users and administers to tell the system who they are and prove that they have permission to access the system (Golding, 2008). This is still widely achieved by having a 'user name' and password, which can be either user or machine generated. This method of identification and authentication has several potential flaws and a more recent development, described by Plaga (2009) as biometrics, makes use of 'intrinsic [human] physical or behavioural features' (p. 447) such as retina scans and fingerprinting which take the place of identification and authentication user names and passwords.

Malicious software comes in many shapes and forms and is usually defined by the means of delivery and intended outcome. For example, a Trojan Horse is normally lines of code hidden within an authorised application with the aim of 'exploiting the legitimate authorisations of the invoking process' (Krutz and Vines, 2003b, p. 925). A virus is self-sustained and will attempt to infect system files and applications, and will normally deliver its malicious payload when a trigger is activated (Krutz and Vines, 2003b). The distinction between a virus and a worm is that, in addition to delivering a malicious payload, a worm can work its way independently across connected networks (Schultz and Shumway, 2002). It is possible to combine the three attributes of Trojans, viruses and worms to make the job of anti-virus software that much more difficult. (See, for example, STUXNET in Piggin (2010).) Anti-virus software, and all the derivatives, also comes in many shapes and forms. However, they all suffer from similar shortfalls including those identified by McAfee (2011):

- Out of date patches for known vulnerabilities to applications and operating systems make antivirus software next to useless
- The antivirus signatures are not updated
- The spread of a virus can outpace antivirus updates

Delivering effective security training and improving security awareness are important countermeasures. Krutz and Vines (2003b) suggests that the starting point for security training at the organisational level is:

1. Policies
2. Standards
3. Guidelines
4. Procedures
5. Technical training
6. Hypothetical security vulnerability scenarios

Krutz and Vines, 2003b, p. 28

Both training and awareness should target the message that not undertaking or following security can lead to problems. Individuals who are not security trained must understand how their actions and inactions can impact on the security of the organisation. Raising security awareness can be achieved by:

- Lectures and presentations
- Electronic self-help presentations
- Posters and newsletters
- Incentives
- Reminders

Krutz and Vines, 2003b, p. 26

Overall, countermeasures can lead to complacency; software can go out of date, and the overall effort may not be cost effective. However, a balanced set of countermeasures which are easy for people to use and maintain are generally accepted as important to maintaining system security. Notwithstanding the limitations of cryptography, firewalls, identification and authentication, antivirus software and security training, and the fact that they are neither the solution for every security

aspect of a networked system, nor the sole sufficient safeguard against network misuse, and despite development trends that threaten them, they still deliver important components of a layered defence. The dangers, characteristics of ICT and security terminology revealed so far are summarised in Table 2.1.

Table 2.1: Terminology that represents dangers to ICT security in a maritime environment
New dangers of the growing reliance on maritime ICT
Lack of awareness of security issues
Problems posed by the complex nature of maritime ICT
Regulation of ICT security in a maritime environment not in place
Issues with virtual private networks
Issues with automated systems
Issues with marine radio and wireless radio
Issues with the loss of distress urgency and safety communications
Unknown impact of incidents
Lessons from military maritime ICT
Eavesdropping
Location tracking
Spoofing
Jamming
Tunnelling and software defined radio and dynamic frequency allocation
Issues with transition from fortress security to cyber security
False sense of security
Issues with layered defence
Need to know verses need to share
Risk based security processes
Security analysis models
The need to understand cyber security in a maritime environment
Countermeasures and layered defence leading to complacency and mistakes

2.4 Sector specific security literature

Life at sea is characterised by Collins and Hogg (2003) which describes seafarers as 'the ultimate distributed workforce' (p. 209) because they work in a 'global industry in continuous operation, without geographical or temporal boundaries, and increasingly reliant on virtual technologies' (p. 210). Their paper does not consider barriers to security *per se* but does note that security constraints and sensitivities stopped them from gaining first-hand experience at sea. By drawing on the work of Baert (1998),

Davies and Parfett (2000) and cross sector work such as Black and Ulrich (1999) and Collins (2002) they review the use of ICT in the maritime sector, mainly the potential for exploiting satellite communications and discuss the pros and cons of personnel management and welfare in the context of distributed international crews. Their recommendations include providing seafarers with better access to ICT including the provision of dedicated computers for training and recreation. Collins and Hogg also point to the need to invest in 'knowledge management to improve remote collaboration' (p. 236) and 'light data' (p.237) methods for down loading maritime distance learning to ships.

The integration of the information sharing systems led the New Zealand Government (1999) to voice concerns over the possible effects of computer software 'bugs' on critical ICT at sea. They commissioned an enquiry into the nature of the systems required to maintain a vessel at sea. The associated report identifies a wide range of ICT dependent systems including: propulsion, electrical generators, stabilisation, steering and damage control. The report also highlights the importance of navigation, radio and safety communication systems.

When describing their deployment of complex systems to warships, QinetiQ (2006) states that 'there is an increasing reliance on networked information technology (IT) in ship-wide and telecommunication systems' (p. 1). At a tactical level, merchant and military vessels need to communicate and Lees and Williamson (2009) describe methods for 'radiocommunications between British merchant ships and HM warships' (p. 191) which includes voice and data and voice. Very High Frequency (VHF) voice circuits are the principle means of 'bridge to bridge' communications and are not encrypted. Sluiman (2010) notes that:

> Vessels transiting the Gulf of Aden receive passage guidance, recommended routing, and threat assessments when they send an initial report to the UK Maritime Trade Operations office in Dubai. However, wireless systems to communicate such unclassified sensitive information to merchant ships do not always provide protection against unauthorized disclosure.
>
> Sluiman, 2010, p. 76

Sluiman goes on to describe the need to encrypt radio with merchant ships so that this threat can be reduced. Data circuits used to communicate between merchant and military vessels use equipment which do have encryption. It is however possible to buy relatively cheap decryption software and Sluiman (2010) claims that, during a trial using such decryption software:

> The software flawlessly decoded the Inmarsat C frames, assembled the messages, and logged them. This effectively means that maritime criminals with no more than a basic knowledge of radio technology and computers can read all Inmarsat C messages sent from an LES [Land Earth Station] after an investment of $3,400 on equipment and software.
>
> Sluiman, 2010, p. 77

It is not unreasonable to suggest that the research reported in this thesis anticipated the findings of the report by ENISA (2011) of their investigation into cyber security in the European maritime sector. Although the ENISA (2011) research only identifies one barrier to maritime ICT security 'the lack of awareness on cyber-risks' (p. 17), the short, medium and long term priorities could point to potential barriers if these priorities are not achieved or are lacking in some way. (See Table 2.2.) For example, several of the ENISA (2011) priorities have been, in past research, flagged as potential barriers. These include: problems with agreeing information exchange between allies (ITU, 2011); inadequate security awareness strategies (Ebrahim and Irani, 2005); and failure to agree roles and responsibilities (Alberts and Dorofee, 2003).

Table 2.2: ENISA short, medium and long term priorities (ENISA, 2011, pp. 19-20) mapped to potential barriers	
ENISA short, medium and long term priorities	Potential barriers
Stimulate dialogue and information exchange	Organisations unwilling or unable to co-operate
Raise awareness about the criticality of this subject	Organisations unsuccessful at raising awareness
Develop strategies and good practice	Strategies and good practice not effective
Develop cyber security training	Poor understanding of the needs of cyber security training
Define roles and responsibilities towards cyber security	Poor understanding of the roles and responsibilities of cyber security
Define and implement a holistic, risk based approach to maritime cyber security	Organisations unwilling or unable to comply
Take appropriate measures in order to add considerations towards cyber in regulatory frameworks governing the maritime sector	Governments unwilling or unable to comply with new regulatory frameworks governing the maritime sector
Develop standards and enforce regulations	Organisations unwilling or unable to co-operate
Develop information sharing and analysis centres	Unable to afford new organisations
Align international and European policies	Unable to achieve agreement on policy alignment
Add cyber to regulatory frameworks in the existing frameworks applicable to the maritime sector	Unable to make the necessary changes to existing frameworks

2.5 Barrier literature

In an examination of enterprise security, Allen (2005) suggests that 'increasing the awareness, knowledge, and understanding of security in an organization is a necessary first step to changing common beliefs' (p. 21). Allen conducted interviews, workshops and conferences in an attempt to 'increase awareness' and 'encourage action to address security at an enterprise level and as a governance concern' (p. 39). The findings identified 'several pervasive barriers that often make enterprise security a daunting undertaking, requiring tenacity and perseverance' (p. 19). A major conclusion of Allen's work is that enterprise security faces 'formidable disincentives to addressing security at more than just a tactical, technical level' including:

> - Security is hard to define and implement
> - Security is not supported by a universal standard
> - Security can be seen as having negative impacts such as cost and inconvenience when implemented, and is usually seen as, at best, avoiding disaster or business impact (cost) rather than providing benefit and competitive advantage.
>
> Allen, 2005, p. 21

In an effort to track how barriers have changed over the years, Chitura *et al.* (2008) set out to determine if the barriers reported in literature on the preliminary take up of e-commerce in the 1990s differ from the barriers reported between 2000 and 2008. To achieve their aim, they conducted a review of the work of Abell and Lim (1996), Lawson *et al.* (2003), MacGregor and Vrazalic (2004), Stanfield and Grant (2003) and other authors. Their analysis provides a range of social, management and technical barriers which are associated with the take up of e–commerce which suggested the range of barriers that existed in the late 1990s still existed in 2008 together with 'a seemingly new breed of barriers' (p. 9).

It is interesting to note that early barriers to take up included 'concerns about privacy and security issues with the use of the Internet' (Chitura *et al.*, 2008, p. 3) and 'concerns about security of e-commerce/payment systems' (Chitura *et al.*, 2008, p. 9) because data security, secure electronic payment systems and on-line banking still cause concerns today. For example, Ball (2010) undertook an exploratory case study to investigate data protection (DP) in a call centre based in South Africa. She cross referenced a series of interviews, observations and secondary data 'in order to identify variation in the way different elements of the employment relationship and DP were described' (p. 299). Of particular interest for this research are her observations of the secure working practices of the call centre work force. Each call worker had ready access to private information and that she 'observed (staff) leaving the building with their diaries, which contained customer details, in the evening' (p. 300). Senior management considered the use of customer data for 'unauthorised purposes' (p. 301) to be an abuse of privilege. However, 'where there was something to be gained (i.e. a sale), a serious DP breach went unpunished' (p. 301). Accidental mistakes

were also observed when call centre workers 'read out personal details to the customer rather than asking them the questions which would confirm what was on the computer' p. 301. This tends to support the argument that people who work within the organisation can pose as significant a threat as those who have unauthorised access to the systems. (For further examples of internal threats to organisations see Wall (2007), Kshetri (2006), and Casey (2000).)

Ebrahim and Irani (2005) undertook work to build a framework for conducting government business over the Internet (e-government) 'to provide an integrated architecture framework for e-government adoption that can address and identify the standards, infrastructure components, applications, and technologies for e-government' (p. 589). This work included a critical analysis of the impact of barriers on such projects to classify 'the barriers that might complicate the implementation of the proposed architecture framework' (p. 589). Using multiple sources including Gefen and Pavlou (2002), NECCC (2000), Robins (2001) and Zeichner (2001), they drew up a list of barriers to security and privacy:

- Threats from viruses, worms and Trojans
- Absence of privacy of personal data
- High cost of security applications and solutions
- Unauthorised external and internal access to systems and information
- Lack of knowledge for security risks and consequences
- Assurance that transaction is legally valid
- Lack of security rules, policies and privacy laws
- Inadequate security of government hardware and software infrastructure
- Lack of risk management security programme
- Unsecured physical access to building or computers rooms

Ebrahim and Irani, 2005, p. 602

Looking in more detail, one of their findings was that 'a barrier frequently cited is the need to ensure adequate security and privacy in an e-government strategy' (p. 603). This barrier manifests as the inadequate provision for computer security, privacy and

confidentiality. Another of their findings suggests that effective security will help 'build citizen confidence and trust in the online services and transactions (pp. 603-604).

Returning to Ebrahim and Irani (2005), they noted the finding of Medjahed *et al.*, (2003) that suggest 'security of infrastructure is still one of the most crucial and least understood issues associated with internet-based communication and applications' (Cited by Ebrahim and Irani, 2005, p. 601). This remains valid today with the emergence of Cloud Computing and Cyber-security where central services and applications make the challenges of data privacy that much harder. (For a description of Cloud Computing security see Krutz and Vines (2010).) From a security perspective, Cloud Computing represents a return to the 'time-sharing model that was widely employed in the 1960s before the advent of relatively lower-cost computing platforms' (Krutz and Vines, 2010, Kindle Locations 290-291). Barriers arising from such systems may have an unrecognised effect and may even apply in ways that are beyond the control of the participants. For example, the ways in which ICT systems are inter-connected may deliver commercial benefits but may also have consequences for security that have not been accounted for. In their cross sector research on the long term economic significance of ubiquitous ICT, undertaken on behalf of the ITU, Fleisch *et al.* (2005) discuss and evaluate the barriers faced by the retail, logistics, automotive and aviation, and pharmaceutical industries and then apply their findings to the telecommunications industry. Amongst their findings is that the provision of data security and data protection is essential if secure transactions and the protection of personal data is to be achieved. They illustrate their point by stating that 'this ubiquitous data becomes both more valuable and more vulnerable, because it allows a very comprehensive picture of a person and their behaviour to be

compiled' (Fleisch *et al.*, 2005, p. 11). They also suggest that without security, the full benefits of ICT will not be realised. Although not concomitant with security, the following barrier may be significant in the maritime ICT environment because of the impact of automation. The threat of 'infrastructure breakdown' when 'many objects can only function properly when connected' (Fleisch *et al.*, 2005, p. 11) points to the possibility that as maritime ICT evolves to achieve a greater integration in a way that is not yet recognised, then failures in one object may have 'knock on' effects on-board and across the maritime sector.

In their review of work from a multidisciplinary research programme, Anderson and Moore (2009) suggests that repeated security failures and the need for diverse organisations to share and interact over virtual systems and infrastructures has forced information security to evolve from the technical discipline of computer science into one that involves experts from many fields. Their information security research programme is combining with economics and psychology in an attempt to gain new insights into traditional information security issues such as 'privacy, bugs, spam and phishing' and 'more general areas of system dependability and policy' (p. 2718). Of all their findings, three are of particular interest for this thesis. The first is that in a virtual network environment 'security failure is caused at least as often by bad incentives as by bad design' (p. 2717). For example, from an economic perspective 'People who connect insecure machines to the Internet do not bear the full consequences of their actions' (p. 2718). They suggest that 'designers can structure interactions to minimize hidden action or make it easier to enforce contracts'. The second are the increasing instances where criminals are turning to the use of 'psychology'. For example, the 'ease with which computer users are deceived by fake websites' (p. 2723).They also

note that 'Insecure software dominates the market for the simple reason that most users cannot distinguish it from secure software' (p. 2723).

It is useful to consider correlations between barriers from research fields that are not explicitly about ICT security but do have sociological, management and technical issues that are relevant to a closed environment on-board ships. For example, using a case study approach, Watts (2010) reviews the barriers to 'higher education distance learning in the prison setting' (p. 1). She highlights the contribution of the Open University's open distance learning model but notes that, the provision of a tutor to help with the on-line material is often missing in prison. Watts also draws on the work of Simpson (2009), Demiray and Sharma (2009), and France and Beaty (1998) to show how difficult distance learning can be. It is not too difficult to extrapolate her conclusions into a maritime environment in which security education and awareness have to be made available anywhere in the world:

- Ships are very stressful places and this negatively affects concentration and study motivation.
- The distraction caused by continuous background noise.
- Routines that lead to restricted opportunities to study.
- Limited or no direct one-to-one support.
- Lack of access to suitable distance learning technology.

Based on Watts, 2010, pp 3-4

Another example, although not concerned with barriers to ICT security as such, comes from Storey and Buchanan (2007).They present a number of interesting social and management barriers that may be relevant to the maritime sector. In their project working paper on patient safety they draw on literature and their own empirical research in eight acute hospitals in the UK to identify six barriers caused by professional 'close shops'. For example, they use five barriers identified by Amalberti and Auroy (2005) the first of which is caused by 'performance and productivity focus'

(p. 11). This is relevant to the maritime sector because of the pressures imposed by demanding delivery and turn around schedules. Their next barrier 'professional autonomy' (p. 11) and the need for checks and balances when professional discretionary powers can override policy is important because life at sea conforms to a strict hierarchy and individuals make mistakes which can in turn can lead to serious incidents at sea. Their third barrier is 'craft worker mind-set' or 'the individual working practice of an 'expert', versus the standardised work practice of the organisation' (p. 13). At sea and away from a central authority, then mariners have to be self-sufficient. As with the health care industry, the challenge here is to embody the best traditions of the service whilst integrating new operating conditions. When things do go wrong, then their barrier 'Over-protection of professionals' (p. 14) can come into play such that if a community on-board is 'close knit' then they may try to cover up incidents which need to be reported. Following on, another interesting barrier is that of 'complacency and the complexity of extant systems' (p. 14) particularly if extrapolated to secure ICT because of the operational and safety implications. Storey and Buchanan add a sixth barrier 'the legitimacy or otherwise of audit and advice' (p. 14). Overly complex rules and regulations can cause confusion and stress and working practice will return to 'old ways' once the audit team leave.

2.6 Barriers: generating key words

A general definition of a barrier is 'an obstacle or circumstance that keeps people or things apart' (Oxford English, 1996, p. 115) and so at the start of this review, a barrier was assumed to be either an obstacle that prevents a secure operating state, or a circumstance of the secure operating state that creates a barrier. However, the literature suggests that barriers are somewhat more complicated than simply

obstacles and circumstances. For example, social and technical issues mix to produce new dangers which have to be dealt with if disasters at sea are to be avoided. This theme will be developed as the research progresses. For now, recalling that the barriers reported in Chapters 1 and 2 are not intended to pre-judge the barriers that may or may not be revealed by the research reported in this thesis, they do give a breadth of topics that will help generate key words that can be used to identify and then focus on barriers that are present in the maritime data. It is anticipated that the differences between ICT barriers ashore and afloat will have similarities and differences that are significant and worthy of further research. Table 2.3 draws together the barriers highlighted in the literature so that the relevance to the maritime domain can be considered in the light of the empirical evidence which emerges from the subsequent research.

Table 2.3: Barriers: Key concepts highlighted in the literature so that the relevance to the maritime domain can be considered in the light of the empirical evidence which emerges from the subsequent research.

Reference	Description
ENISA (2011)	The lack of awareness on cyber-risks.
Allen (2005)	There are formidable disincentives to addressing security at more than just a tactical, technical level. Security is hard to define and implement. Security is not supported by a universal standard. Security can be seen as having negative impacts such as cost and inconvenience when implemented, and is usually seen as, at best, avoiding disaster or business impact (cost) rather than providing benefit and competitive advantage.
Chitura *et al.* (2008)	An announcement of data loss can lead to damage of confidence. External attacks on critical infrastructure and the proliferation of cyber-crime. Conflict between security and 'open system' architecture as new business opportunities increase threats and vulnerabilities. Security technology can be rendered ineffective by a failure to differentiate among critical information assets, poorly designed operating procedures or lax attitudes towards security within an organisation.
Ball (2010)	Threats posed by outsourcing. Internal threats to an organisation.
Krutz and Vines (2010)	Cloud Computing security issues.
Storey and Buchanan (2007)	Performance and productivity focus. Professional autonomy or the need for checks and balances when professional discretionary powers can override policy. Craft worker mind-set or the individual working practice of an 'expert', versus the standardised work practice of the organisation. Over-protection of professionals or the need for scrutiny of individuals. Complacency and the complexity of extant systems. The legitimacy or otherwise of audit and advice.

Continued ....

Medjahed *et al.* (2003)	Inter connected network issues critical but not understood.
Ebrahim and Irani (2005)	Threats from hackers and intruders. Threats from viruses, worms and Trojans. Absence of privacy of personal data. High cost of security applications and solutions. Unauthorised external and internal access to systems and information. Lack of knowledge for security risks and consequences. Assurance that transaction is legally valid. Lack of security rules, policies and privacy laws. Inadequate security of government hardware and software infrastructure. Lack of risk management security programme. Unsecured physical access to building or computers rooms.
Fleisch *et al.* (2005)	Lack of data security. Lack of privacy. Loss of confidence due to security incident. Infrastructure breakdowns when many objects can only function properly when connected. Social exclusion when ICT is not available to all. Incorrect automated decisions and the damage they can cause.
Anderson and Moore (2009)	People who connect insecure machines to the Internet do not bear the full consequences of their actions. Insecure software dominates the market for the simple reason that most users cannot distinguish it from secure software. The ease with which computer users are deceived by fake websites. Many people say they value privacy yet act otherwise when online. The societal misperceptions of risk. Why is it, for example, that most people care too little about online security and privacy, yet overreact to terrorism?
Watts (2010)	Insufficient ICT to support distance learning. (Ships) are very stressful places and this negatively affects concentration and study motivation. The distraction caused by continuous background noise. Routines that lead to restricted opportunities to study. Limited or no direct one-to-one support.
Collins and Hogg (2003)	Lack of access to ICT for seafarers. The need for dedicated computers for training. Invest in knowledge management to improve remote collaboration. Invest in 'light data' methods for down loading maritime distance learning to ships.
Sluiman (2010)	Lack of security on voice circuits. Weakness of encryption software. Poor security operating practice by service providers.
Roumboutsos *et al.*(2005)	Attacks against maritime targets ashore
Dunlop and Smith (1994) Goldsmith (2005) Rackley (2007)	Limitations of using EM spectrum.
Gaitskell (1998) Clark (1997) Mann (2008)	Eavesdropping.
Rishi (2005) Smith (1998) Luo *et al.* (2011) NATO (2010)	Location tracking.
NATO (2010) Anderson and Moore (2009) Pfleeger (1997)	Spoofing.
Schneier (2000) Smith (1998) Rackley (2007) Leon *et al.* (2010)	Jamming (Denial of Service).
Hill (2000) Kalsson (2011)	Tunnelling.
Piggin (2010)	Adaptive malicious software (For example, Stuxnet).
ITU (2011)	International legal measures do not allow crime committed across borders to be successfully prosecuted. Technical and procedural measures cannot prevent, detect and respond to attacks Organisational structures inadequate to prevent, detect and respond to attacks. Inadequate knowledge and expertise of cyber security. International co-operation, dialogue and co-ordination cannot be achieved.

Continued ....

Internet Engineering Task Force (2007)	Human error. Deliberate trespass. Theft. Natural causes. Technical failure. Technical obsolescence.
Pleeger (1997) International Organization for Standardisation (2008) Piggin (2010)	Need to know verses need to share.
HMG (2007) Alberts and Dorofee (2003) Caralli and Young (2008)	Risk based security processes and security analysis models.
Clark and Knake (2010)	The need to understand cyber security.
Whitman and Mattord (2007) Schneier (1996) Schneier (2000) Van der Lubb (1998) CESG (2008) Open University (2008)	Countermeasures and layered defence leading to complacency and mistakes.

2.7 Conclusion

The body of literature dealing with maritime ICT security is not substantial but there is a significant amount of literature examining ICT security in other contexts that is relevant to this work. It has thus been possible to identify a range of potential barriers that can be taken forward for consideration. Drawing on the results of this literature review enables the following research questions to be formulated:

1. How are mariners responding to the increasing use of ICT and how and to what extent is their security behaviour adapting to the changes in technology?

2. What has been the impact of ICT on maritime organisations' security culture?

3. How have maritime authorities and organisations responded to the potential threats and vulnerabilities of maritime ICT?

4. Can the barriers be used as the basis for a secure ICT profile that can be used successfully in a maritime environment?

The next chapter will describe the research methodology and analysis used to progress this research.

Chapter 3

Investigating the barriers to ICT security in a maritime environment: research method, analysis and implementation

3.1 This research: purpose and background

Chapter 1 identified the operational and ICT security aspects that are important to mariners. Although examination of the literature revealed only limited historic research on ICT security in the maritime setting, the literature review reported in Chapter 2 revealed a rich body of research in the allied area of security in a non-maritime (but relevant) setting. For example, the security dangers faced by shore side Virtual Private Networks and wireless radio have been examined in some detail. Upon closer examination it became apparent that this rich understanding has evolved from the reporting and analysis of successive ICT security incidents with roots dating back to the 1988 'Internet worm' (Casey, 2000, p. 209). However, specific literature about the security dangers faced by ship board ICT and the way in which ship board ICT, maritime radio and shore infrastructure now interact in real time is not readily available. The review also looked at barriers to ICT security to identify key concepts that are most likely to be relevant to ICT security in the maritime sector. For this, a general definition of a barrier 'an obstacle or circumstance that keeps people or things apart or prevents communication' (Oxford English, 1996, p. 115) was used to begin to identify the nature of barriers.

The literature suggest that real world barriers are a complex mix of technical and social issues and that any barrier can display characteristics that depend upon

objective and subjective viewpoints. The barriers assembled from the literature as set out in Table 2.3 are representative of the broad range of potential barriers faced by mariners using ICT in a maritime environment. The remainder of this chapter presents the research methodology used to investigate the barriers in 'real world' maritime organisations and the logic underpinning the methodology decisions.

3.2 Research methodology

The research methodology is designed to provide a robust yet flexible approach to investigating the barriers to ICT security in a maritime environment so that the emergent barriers can be used to develop a secure ICT maritime profile that will be capable of being updated on an on-going basis.

The barriers to ICT security that are being explored in this research result from the combination of complex technical issues with complex social issues in a maritime environment. There is the need to explore mariners' experiences of ICT use at sea whilst recognising that their beliefs, behaviours and values can be just as important and relevant as the properties of the ICT that they use. 'Objective' and 'subjective' research are often presented as opposites but neither captures the complexity of the maritime security situation or the balance required between technical and social issues.

Corbin and Strauss (2008) suggest that both objective and subjective viewpoints have their advantages and disadvantages and indeed, at times they do actually both make use of the same techniques. Fortunately, there exists a half-way point between the extremes of objective and subjective where, as Eastery-Smith *et al.* (1991) suggest, a researcher can find a 'contextual field of information' (p. 25). It is this contextual

field of information that this research will seek to examine as it tries to identify barriers. Exploratory studies such as those described by Blumer (1969) offer several advantages for this research, especially in the absence of a body of directly relevant maritime literature. One important advantage is that it will allow the researcher the freedom to ask questions and review multiple sources of data, whilst maintaining an open mind to seek new insights (Saunders *et al.*, 1997).

Qualitative data gathering was an important element of the research methods deployed. Miles and Huberman (1994) suggest that one of the strengths of qualitative data is that it can 'focus on naturally occurring, ordinary events in natural settings' (p. 10). To give a depth of understanding rather than a superficial breadth, interviews rather than survey methods were selected (Saunders *et al.*, 1997). To achieve this depth of understanding of the real world experiences, information was gathered during one-to-one semi-structured interviews with Royal Navy related personnel involved with the provision and use of ICT. The interviewees' knowledge of ICT is relevant for three main reasons. First, from a historical perspective, they will have witnessed ICT evolve both at sea and on land. As such, they are likely to be able to share their insights into good and bad practice. Secondly, from their current operational perspective, they will know how ICT is being used in a range of situations. In this sense, they may not have the answers to problems but they should have suggestions about what might constitute solutions. They will also be privy to that which Potter (2006) refers to as 'grey literature' (p. 168) and/or data that is not in the public domain but that may be important to this research. Thirdly, from a future perspective, their knowledge of proposed new ICT could be invaluable in informing the direction work to build the proposed security profile needs to take.

The interviews were semi structured to allow emerging ideas to be explored and 'to clarify your understanding of a problem' (Saunders, 1997, p. 78). Walsham (2006) suggests that during the interviewing process the role of the researcher can range from 'neutral observer' to 'a full action researcher' (p. 321). For this research, the researcher assumed the role described by Silverman (2000) as an 'empathic observer' a mid-way point between the neutral observer and full action researcher described by Walsham (2006).

Having identified the field of information and established the data collection method, the next step was to establish the method of data analysis. Miles and Huberman describe analysis thus:

> To review a set of field notes, transcribed or synthesized and to dissect them meaningfully while keeping the relations between the parts intact, is the stuff of analysis. This part of analysis involves how you differentiate and combine the data you have retrieved and the reflections you make about this information.
>
> Miles and Huberman, 1994, p. 56

The emergent themes drawn from the interview transcripts are assigned to categories and concepts much like the coding described by Miles and Huberman (1994). Corbin and Strauss (2008) suggest that:

> A researcher can think of coding as "mining" the data, digging beneath the surface to discover the hidden treasures contained within data.
>
> Corbin and Strauss, 2008, Kindle Locations 1019-1027

In the context of this research, analysis can be seen as an attempt to make sense of the data whilst being mindful that prior to analysis, the interview questions have already undergone a series of encoding and decoding. For example, Foddy (1995) notes that 'researcher encodes question, respondent decodes question, respondent

encodes answer and researcher decodes answer' (drawn from Foddy (1995), Figure 3.1, p. 26). The coding for the analysis of the Royal Navy data started by summarising the data from each interviewee. Next, the broad range of key terms drawn from the literature were used to focus the data and so make the range of categories 'progressively narrower as the research progresses' (Saunders *et al.*, 1997, p. 79). A tabular representation of the interviewee's opinions was then built and structured to reduce the complexity of the subject matter and enable the emergence of themes arising from the research data. The resultant categories were combined into related concepts; links between concepts identified, and interpretive coding used in an attempt to integrate all the threads of this research. An interpretive view of the result of such analysis is offered by Geertz (1973) 'what we call our data are really our own constructions of other people's constructions of what they and their compatriots are up to' (p. 9). The interpretations are founded on personal experience, the literature and other source and data from Royal Navy interviews, whilst being mindful of Corbin and Strauss (2008) who note that 'in the end only the data themselves are significant, but it helps to have a little insight to start with' (Kindle Locations 598-600).

There are many options when it comes to justifying the methodology chosen for this research. For example, Yin (2003) suggests that it is possible to 'judge the quality of any given design according to certain logical tests' (p.33). He goes on to describe four tests that are relevant across the social sciences but only three are applicable to this research:

1. Construct validity: establishing correct operational measures for the concepts being studied.
2. External validity: establishing the domain to which a study's findings can be generalised.

3. Reliability: demonstrating that the operations of the study – such as the data collection procedures – can be repeated with the same results.

Yin, 2003, p. 34

To meet the construct validity test, this thesis has drawn on a wide range of literature and data in an attempt to provide 'convergent lines of enquiry' (Yin, 2003, p. 36). Also, this thesis provides an accurate record of the research undertaken. To meet the external validity test, concepts and implications are derived which are intended to apply beyond the immediate research focus. To meet reliability criteria, the design of this research has been deliberately chosen to make it relatively straightforward to follow. Yin (2003) makes the point that the purpose of reliability is to be able to replicate the research but not the results *per se*.

A compelling work on making research appealing and convincing is that of Golden-Biddle and Locke (1993) who describe three criteria:

1. Authenticity – appeal to readers to accept that the researcher was indeed present in the field and grasped how the members understood their world.
2. Plausibility – make claims on readers to accept that the findings make a distinctive contribution to issues of common concern.
3. Criticality - endeavor to probe readers to re-examine the taken-for-granted assumptions that underly their work.

Golden-Biddle and Locke, 1993, p. 595

Walsham (2006) describes authenticity as a demonstration 'that the authors have 'been there'' (p.326). Prior to this research, the author spent 14 years at sea and a further 11 years working in maritime headquarters. During this research, the author visited the Portsmouth site regularly and was involved with various maritime ICT projects. The distinctive contribution made by this research is described in Chapter 7, but in summary the research provides an updateable maritime ICT profile that can be used by military and commercial organisations. Finally, it is intended that this

research will challenge the maritime sector to rethink their current lack of awareness of maritime ICT security issues.

3.3 Refining the techniques and procedures

Having established the methodological approach for the data collection, the next step was to refine the techniques and procedures for gathering the data (Saunders *et al.*, 1997). A scoping exercise was developed to assess interest in this research topic, establish contact with potential interviewees and to alleviate concerns that exist about the sensitive nature of security issues. Royal Navy contacts were approached in Portsmouth and London and asked to act as intermediaries to help establish contact with potential interview candidates. A 'neutral observer' (Walsham, 2006, p. 321) stance was taken throughout the exercise.

3.3.1 Pilot interview

The scoping exercise was undertaken at the Portsmouth and London sites between the 23rd and 27th of February 2009 culminating with a pilot interview in London on the 27th February 2009. Preliminary questions designed to consider the idea that barriers are obstacles to progress were developed to inform the pilot interview. The questions were based on the material set out in Chapters 1 and 2, and designed using ideas from Foddy (1995), Miles and Huberman (1994), Potter (2006) and Carnegie Melon Institute (2007). Kvale (1996) has identified nine types of question asked in qualitative interviews and these were used to think about the types of questions and how they might best be framed.

- Introducing questions: 'Why did you...?' or 'Can you tell me about...?' Through these questions you introduce the topic.

- Follow up questions: Through these you can elaborate on their initial answer. Questions may include: 'What did you mean...?' or 'Can you give more detail...?'
- Probing questions: You can employ direct questioning to follow up what has been said and to get more detail. 'Do you have any examples?' or 'Could you say more about...?'
- Specifying questions: Such as 'What happened when you said that?' or 'What did he say next?'
- Direct questions: Questions with a yes or no answer are direct questions. You might want to leave these questions until the end so you don't lead the interviewee to answer a certain way.
- Indirect questions: You can ask these to get the interviewee's true opinion.
- Structuring questions: These move the interview on to the next subject. For example, 'Moving on to...'
- Silence: Through pauses you can suggest to the interviewee that you want them to answer the question!
- Interpreting questions: 'Do you mean that...?' or 'Is it correct that...?'

Kvale, 1996, pp. 133-135

The pilot interview (SY1) was recorded on disc, with the interviewees' permission. Walsham (2006) notes the advantages and disadvantages of tape recording interviews. These are summarised in Table 3.1. One additional advantage with digital media is the availability of software that, notionally, converts recordings into text. However, the overriding impression was that although the potential candidates expressed willingness to be recorded they actually appeared 'uncomfortable' with being recorded when they were speaking so the practice of tape recording was discontinued for the main interviews.

Table 3.1: Advantages and disadvantages of tape recording interviews (Walsham, 2006, p. 323)

Advantage:	Disadvantage:
• Truer record of what is said compared with taking notes. • It is possible to return to a transcript later for alternative forms of analysis. • It is useful for picking out direct quotes. • It frees the researcher to concentrate on engaging with the interviewee. • It is popular with neo-positivist reviewers.	• It is very time consuming. • May make interviewee less open or less truthful. • Tape-recording does not capture the tacit, non-verbal elements of an interview, which are crucial aspects of the experience for the researcher.

Four conclusions were reached as a result of the scoping exercise. The first is not surprising; those who participated in the informal discussions made it clear that security is a sensitive topic and needs to be handled accordingly. The Assistant Chief of Staff of the Communications and Information Systems Division stated that he was happy to allow access to personnel and documentary material with the caveats that the chosen personnel were willing to take part in interviews and that any documents used had to be unclassified. To meet these stipulations, all contacts with personnel were preceded by an explanation of the nature of the research and the thesis itself contains no material that can identify specific vulnerabilities of any individuals or organisations. Secondly, whilst the informal discussions suggested that an understanding of security barriers as firewalls does exist, the concept of barriers to secure ICT proved to be less well understood. To help the situation, the pilot interview questions were refined to help obviate some of the issues associated with the use of security terminology. Thirdly, the informal conversations revealed a common concern relating to the introduction of the HMG Information Assurance Maturity Model (CESG, 2008b). The purposes of this model, designed in partnership with the Central Electronic Security Group (CESG), are to improve awareness of information security issues across all HMG Departments and to mitigate the widely-publicised losses of personnel information. (For examples of these losses see Burton (2008) and Hannigan (2008).) The questions used in the pilot interview were modified to probe the incidents which lead to the introduction of the Information Assurance Maturity Model and the impact on the Royal Navy. Fourthly, the informal discussions revealed the fact that unlike people in very many other settings, Royal Navy personnel (circa 2009) do not use the term ICT in normal circumstances. As a consequence the interview data contains abbreviations and such as CIS (Communications and

Information Systems) which can be used when referring to either the CIS Branch of the Royal Navy or when referring to CIS as an operational capability. Other examples include NEC (Network Enabled Capability), IT (Information Technology), and a range of terminology such as 'Formal Messaging' which refers to the Royal Navy's primary Command and Control communications system that provides secure text based messaging between headquarters, establishments and ships. For the purposes of this research the acronyms and terminology are grouped under the heading of ICT. Within this chapter and Appendices A and B these terms are explained as they arise and are also tabulated in the 'Acronyms, abbreviations and maritime specific terminology' section at the start of this thesis.

3.3.2 The interviewees: Criteria for selection

The selection of the interviewees was based on the desire to gather data from a cross section of personnel that was as representative as possible of the ICT community (Saunders, 1997, p. 78) and possess a variety of different skills and experience. Following a short discussion with the Assistant Chief of Staff for CIS, approval was received to use the Royal Navy Staff Directory to identify the current incumbents in the posts that would most likely meet one or more of the following criteria:

- Sea going experience to help understand the situation where possible
- Senior management to gain a management perspective
- Experience in security or training delivery
- Experience in current or previous security roles
- Experts from the RN communications and information systems (CIS) including intelligence
- Consultants who support the Royal Navy
- Any experience using ICT at sea or on land

By reviewing MODUK documents, reference material and other sources, a career profile of the potential interviewee population was built. For example, Civil Servants, including those serving in the Ministry of Defence, can elect to follow a security-based career path and as such they receive dedicated security-related training for their jobs. (See, for examples of Information Security Competencies, Cabinet Office (2005).) However, the Royal Navy has no specific ICT security branch and so officers and ratings are temporarily attached to security jobs from their parent branches. This introduces an interesting dimension of continuity when considering the scope of Royal Navy security jobs. The Royal Navy Intelligence Branch was disbanded in 1990 (INT2), but following the terrorist attacks in America in 2001 and the subsequent increase in the perceived need for intelligence officers generally, work was in hand to re-form the specialisation in 2009. (The Royal Navy Intelligence Branch was re-formed in 2011.) Between 1990 and 2011, however, officers were appointed to carry out intelligence jobs on an ad hoc basis in a similar fashion to those working on security. Another relevant area is the RN Weapons Engineering Branch. This has undergone several changes over the last fifteen years. For example, during the 1990s the Weapons Electrical Branch was merged with the CIS Branch but the result was not widely acknowledged as successful and the two branches were de-merged in 2009. Potential interviewees in this area were those who represented a range of experience including systems engineering afloat and ashore, project management, teaching and general management responsibilities. Potential interviewees representing the CIS Branch were a mix of Civil Servants and Royal Naval personnel. Their job descriptions were wide ranging, taking in anything from a project manager to front line support or systems design and implementation. The Civil Servants tended to have relatively long tenure in post whilst Royal Navy officers and ratings could expect

to be in post for anything from one to three years. All the jobs mentioned in this section can also be filled by retired personnel recalled to duty or by Maritime Reservists. (Further information on the conditions for Full Time Reserve Service personnel is available via MODUK (2010a).) To enrich the overall field of data, civilians who work for the Royal Navy and MODUK as external consultants were also invited to take part. Interviewees in this category had a mix of Merchant Navy, military and commercial experience in information management and security fields.

After a review of the data collected during the scoping exercise, a return visit was made to the Portsmouth site. 27 candidates were approached directly or by telephone and asked if they would agree to take part in the research. 18 agreed to be interviewed, of whom 3 subsequently withdrew. The 15 personnel who were interviewed are listed in Chapter 4, p. 66, Table 4.1, where they are grouped into five categories based on the Royal Navy branch structure in Table 3.2. Several of the prospective interviewees indicated that the views they were expressing were their own opinions and did not necessarily represent the views and behaviour of the Royal Navy, MODUK or any other maritime organisation. With one exception (INT1), the interviewees stated that they were willing for their opinions to be reported. After a short discussion, INT1 agreed to be quoted anonymously. The interviews were conducted in London or Portsmouth. The high level Command structure of HMG, MODUK and Royal Navy is given in Table 3.3 to help situate the research by showing where the interviewees work and their security responsibilities.

Table 3.2: Summary of interviewee sorted by career categories		
Career category	Number in career category	Identification range
Security experts (MODUK and RN ICT security personnel)	3	Sy1 to Sy3
Intelligence (RN intelligence analysts)	2	Int1 and Int2
Engineering and education (RN electrical and electronic engineering and education)	4	Eng1 to Eng4
Communication and Information Systems (CIS) (The management and implementation of CIS capability)	3	CIS1 to CIS3
External consultants (Those who support the RN and MODUK)	3	Con1 to Con3

Table 3.3: Command structure: the hierarchy of HMG, MODUK and Royal Navy			
Organisation	Security responsibility	Reports to	Situation circa 2013
HMG	Creates legal statutes Directs Departments of State (including MODUK)	Electorate	Labour government replaced by coalition government in 2010. Widespread redundancies underway across the MODUK.
Ministry of Defence London site	Sets MODUK security policy Monitors progress Arbitrates disputes between Military Commands	Reports to HMG	Reports to HMG
Fleet Headquarters, Portsmouth site (Renamed Navy Command Headquarters in 2010)	Enacts MODUK security policy. Modifies security policy for maritime environment	Reports to MODUK	New 2013 Command structure devolves certain powers down to the three military Commands
Ships and establishments worldwide	Enacts Royal Navy security policy and other security policies for joint operations	Reports to Fleet Headquarters on RN issues. Reports to Joint Headquarters Northwood for joint operations	Fleet Headquarters Portsmouth renamed Navy Command Headquarters in 2010

3.3.3 Major modifications based on the findings of the scoping exercise

Several major modifications to the draft interview schedule were made as a result of the scoping exercise. First, it had been intended to use a diagram of MODUK security functions with the aim of helping the interviewees understand the context of the questioning. However, following the informal discussions, it was decided not to use

the diagram because of the danger it would encourage interviewees to focus on specific security issues and thus risk 'leading the interviewees' (Foddy, 1995). Second, it was decided to refine the wording of the interview questions. In this way, it was intended to make the topics understandable by using their own terminology (such as ITSy and CIS in place of ICT) whilst allowing the interview questions to remain flexible, and the interviewer to probe for barriers. Also, 3 questions (Questions 4, 5 and 6) were added to probe the issues surrounding information handling and the Information Assurance Maturity Model. Follow on questions drawn from Miles and Huberman (1994) were kept to hand to help probe interviewees' responses. To reflect these changes and to help with data storage and retrieval, the questions were re-grouped under the four new headings: environment; technology; systems failure; and systems management. (See Table 3.4.) The final major modification was instigated because of the sensitivity of this subject. As Walsham (2006) notes, 'One is often unsure about potential harm to participants, cannot always enable fully formed consent, do sometimes invade some elements of privacy, and may 'deceive' about the precise aim of one's research' (p. 327). To alleviate concerns of this nature, the researcher drew together information from Royal Navy (2009) diversity and equality documents and Reynolds (2003) guidelines on information technology ethics to produce a set of personal research guidelines. A copy was e-mailed to each interviewee prior to the meeting. The guidelines are supplied at Appendix A. Participants were assured that their anonymity would be respected and permission to use their data was obtained from all interviewees' prior to the interviews. One final observation, as Preece (1994) points out, establishing trust is important but 'should not lead to the interviewee being encouraged to give the answers they believe the interviewer wants and so obscuring the true situation' (p. 87). Every effort was made

to avoid the researcher's own thinking taking precedence over the interviewee's opinions (Silverman, 2000). The questions used to guide the semi-structured Royal Navy interviews are supplied as Table 3.4.

Table 3.4: Interview and follow on questions used to start and maintain the flow of the 'semi-structured interviews'

1. In your opinion, does working and living at sea present challenges which are different to other environments?
2. If we were at sea today how do you think we would be using information and technology?
3. In your view, to what extent will new information technology capability play a role in maritime activity?
4. Please name three characteristics that sum up the use of information in your organisation
5. In your opinion, does your organisation consider information to be an important asset
6. What changes to Information Assurance have taken place recently?.
7. From your experience, please describe the likely impact of a temporary or permanent loss of maritime information and technology capability?
8. Will future maritime network capabilities lead to new security threats and vulnerabilities in IT systems?
9. If so, what role could ITSy and systems failure methodologies play in protecting maritime assets?
10. In your opinion, is poor understanding of security practice a continuous cause of security incidents?
11. How will ITSy risk management evolve in a maritime environment?
12. Will accepting cumulative risk have adverse consequences on ITSy in a maritime environment?
13. Are you aware of any more general security methodologies which could be applied to maritime IT?
14. If so, to what benefit?
15. How are the electronic and physical security threats and vulnerabilities faced by maritime systems any different to their terrestrial counterparts?
16. How do you think electronic and physical security threats and vulnerabilities will change with time as new network technology is deployed?
17. a. Can terrestrial IT and systems methodologies be successfully applied in a maritime environment? Or
    b. Will new maritime technologies require new IT and systems failure methodologies?

Follow on questions, drawn from Miles and Huberman (1994):

- *"Have you thought about .....?"*
- *"Why?"*
- *"In what way?"*
- *"For instance, give me an example."*
- *"What caused .....?" (Casual antecedents).*
- *"What was the purpose in doing ...?" (Goal antecedents).*
- *"What happened after ....?" (Casual consequences).*
- *"How do you mean that?"*
- *"Tell me more about that."*
- *"Anything else?"*
- *"How was it possible for 'the interviewee' to do ..." (Enabling factors).*

Miles and Huberman, 1994, p. 24

3.4 The Royal Navy interviews: Data handling

Immediately after each interview, the written notes were typed into Word™ documents. On completion of the write up, two parallel activities were undertaken. First, for the London interviewees, the documents were e-mailed to their work addresses, followed by telephone calls to each interviewee to confirm the accuracy of their own document. Second, a return visit was made to the Portsmouth site in

November 2009 and each interviewee's own documents were discussed face to face to confirm the accuracy of their own document. All the interviewees (London and Portsmouth) were given the opportunity to comment on the content and accuracy of their own document. With one exception, all the interviewees agreed to the accuracy of their own document. One interviewee (INT1) pointed to a sensitive subject that had been recorded in their document. Following a short discussion, the detail of the subject was removed from their document. Once this activity had been completed, the document texts were imported into an Excel ™ spread sheet in preparation for the analysis phase. The spread sheet was structured to reduce the complexity of the subject and allow the barriers relevant to this research to emerge in a form that could be readily used in the design of the updateable maritime ICT security profile. Coding for analysis of the Royal Navy data started with summaries of the interviews. These are set out in Chapter 4. Three interviews were cancelled. The first of these was planned to be with a US naval officer, who was working as a liaison officer with the Royal Navy but he had to return to US before the scheduled interview. The other two were with a German naval officer and a MODUK Civil Servant but both were cancelled by the intended interviewees due to pressure of work.

3.5 Additional data: The Merchant Navy

One of the advantages of exploratory research is the freedom to consider aspects which may not be immediately obvious to the subject (Saunders *et al.*, 1997). Researchers taking a positivist approach may consider deviations from the main aim as showing a lack of direction (Easterby-Smith *et al.*, 1991). However, it was decided to undertake a parallel activity to that of the Royal Navy data collection, in an attempt

to gain an understanding of the ISPS Code, which although a physical security risk assessment could be helpful in this research. Additional data was collected from Merchant Navy officers when the researcher undertook a 'Proficiency as Ships Security Officer' course. The purpose was to gather data from Merchant Navy officers relating to their practical experiences with security at sea. Special emphasis was placed on gathering their opinions of the ISPS Code in order to determine the validity and utility of the Code to help build the proposed updateable maritime ICT security profile. Preece (1994) argues that informal conversations offer 'a better indication of a respondent's true attitudes' (p. 120) but also warns that care must be taken not to deviate too far from the topic in hand. Observations were made during the interactions between the attendees and the course leader. The purpose was to identify key security issues that arose. The attendees raising the issues were then approached during break periods and asked to comment on their ideas and to confirm that they would be happy to be cited. Written notes were taken during the course with the permission of the course leader and the attendees. The notes were recorded in a single document but the final document was not circulated to the attendees.

The Merchant Navy notes are used to describe the emerging issues of physical security and incidents at sea that could be used in scenarios in the absence of data on secure ICT maritime incidents. In a parallel activity, a review of maritime incident data from secondary sources was undertaken to try to reveal the potential threat actors and impacts that can be used to inform the updateable maritime ICT security profile. The subsequent data and the results of the analysis are described in Chapter 5.

3.6 Drawing together the threads and practical application

This research was intended to investigate barriers to ICT security and to help in the real world in terms of informing attempts to counter actual and potential dangers. To achieve this, it is intended to draw together the threads of this research into an updateable maritime ICT security profile using the ISPS Code as a reference point and OCTAVE for ICT structures. To satisfy formal security requirements, the profile contains an analysis part and a management part. Barriers were used to inform the formal evaluation and management parts of the profile, and act as guidelines for use by non-security personnel. Updates will be provided using Horizon Scanning methods. Overall it is intended to provide a new understanding of barriers that will help mariners conduct their day-to-day operations safely and securely. These topics are described in detail in Chapter 6.

3.7 Monitoring information from multiple sources

The literature and other sources of information were monitored throughout the period of this research to help keep abreast of current developments in the maritime sector including ICT and security. This information was used to supplement the data collected from literature and interviews and to act as data triangulation points. Triangulation, in this instance, is not used to point to a fact as described by Yin (2003) but rather, to indicate that a number of independent sources are agreeing or disagreeing in some way and so highlight that a noteworthy theme may exist (Savory and Fortune, 2013).

3.8 Conclusion

This chapter has described the methodology by which this thesis attempted to build on the general literature and other papers reported in Chapters 1 and 2 so that the 'real world' barriers to secure maritime ICT can be explored and the results used in the design of an updateable maritime ICT security profile. The next chapter will report the findings of the Royal Navy interviews and present the results of the subsequent analysis.

Chapter 4

Royal Navy: Data, analysis and preliminary findings

4.1 Introduction

As explained in Chapter 3, a series of 15 interviews were conducted with Royal Naval related personnel in London and Portsmouth between February and September 2009 in order to gain an insight into real world barriers to ICT security in the maritime environment. This chapter sets out the data gathered and presents analyses of it.

4.2 Summaries of the interviews

Table 4.1 shows a brief description of each of the people interviewed and provides a pseudonym for each interviewee in order to be able to refer to each interviewee whilst preserving anonymity. In this sub-section each interview will be summarised in turn.

Table 4.1: Summary of the interviewees

Interviewee pseudonym	Background of the interviewees (Notes from each interview are supplied in column 2 of the table in Appendix B)
SY1	A Civil Servant, responsible for the Department's (MODUK) Information Security policy
SY2	A Royal Navy officer serving in IT security with over five years' experience in this subject
SY3	A Royal Navy officer filling a security role for two years
INT1	A Royal Navy intelligence officer with 25 years' experience in MODUK
INT2	A Royal Navy Intelligence Surveillance Target Acquisition and Reconnaissance (ISTAR) specialist with over twenty years' experience
ENG1	A Royal Navy engineer with 20 years' experience in ship systems management and project management
ENG2	A Royal Navy engineer and education officer with 16 years' sea going and shore based experience
ENG3	A Royal Navy Weapons Electrical Officer with 14 years of experience in submarines
ENG4	A Royal Navy officer with over twenty years of education and management experience
CIS1	A senior Civil Servant, working in information systems support
CIS2	A Royal Navy officer with over twenty years' experience in RN, Joint and NATO CIS and engineering
CIS3	A Royal Navy officer with over 12 years' experience of CIS capability development
CON1	A civilian employed as a project manager and is a former Merchant Navy Radio Officer
CON2	A civilian security consultant working on HMG's Information Assurance Maturity Model
CON3	A civilian information management consultant with over twenty years of experience in the subject

SY1 is a Civil Servant with over 15 years of experience in MODUK security and is responsible for setting the Department's information security policy. A pre interview 'chat' with SY1 was most informative, including several off the record remarks which suggested that the MODUK has a certain way to go to achieve effective security in a networked environment. In the interview itself, SY1 described an emerging real time information exchange environment. In this environment, formerly standalone systems are working together to provide everything from safety at sea, to new methods of reducing operating costs. SY1 expressed concern that the impact of the loss of these systems has not been fully thought through. Also, legacy 'manual' skills are no longer taught and there is an over reliance on satellite technology. The potential consequences of an attack against GPS was cited; specifically, the potential impact in a military context that could lead to the loss life, and in a business context that could result in a company having to file for bankruptcy. In SY1's opinion, problems faced afloat and ashore will be similar. However, special consideration has to be made for the corrosive effect of salt water, working conditions, and availability and compatibility of spares. Whist discussing network-enabled capabilities, SY1 cited obstacles including: atmospheric limitations; time needed to download software patches; fall-back procedures if the 'Home' network is under attack; additional burden on staff; and increased opportunities for an adversary. SY1 suggested that the threats will be the same both afloat and ashore. Threat Actors are both internal and external to the organisation. SY1 appeared to favour a security risk management rather than a risk avoidance approach to the problems faced by the MODUK by stating that 'We need to be firmly embedded in business; we need to have a good understanding of business, and the business needs to understand where we are coming from'. In considering what needs to be protected SY1 cited both the workforce and information.

Security needs to be 'built in' rather than 'bolted on at the end of a project' which is claimed will have a disproportionate cost. Whilst discussing security risk, SY1 stated that 'I am not sure whether businesses fully understand that the individual risks they are carrying may have an impact on somebody else. At senior level I am not sure they understand the cumulative effect'. Following a short discussion on standards, SY1 stated that 'The security controls within the MODUK would fully meet and exceed the ISO 27000 controls and this has been so for many years. It has been said that the ISO standard is catching up'.

SY2 is a Royal Navy officer, who appeared to be annoyed at being asked questions about security. However, as the interview progressed, the interviewee relaxed and the value of the answers improved. Overall, the interviewee was of the opinion that the RN and MODUK have the right security processes and practices in place. However, the (MODUK) security manual is considered to be large and unwieldy by the community that use it. The reaction to security breaches in 2007/2008 may have been inappropriate and the changes to accounting and tracking that were implemented could have been more effective. When considering operations, the interviewee suggested that there are no new threats but changing 'threat actors' and the associated security vulnerabilities need a more 'holistic approach' and a better understanding of security by all players. The interviewee cited the nuclear firing chain as an example of potential operational compromise which could have devastating consequences. Because of the critical nature of information and systems, the interviewee suggested that there is a need for ships to be able to work without links to UK or other commands. When asked about cumulative risk, the interviewee was of the opinion that Navy Command risk management can be 'ill judged' suggesting that the information needed for informed risk management is not always available. Other

key words used by the interviewee but not included in this summary are: Protective Marking; Impact Table; Automatic Information System (AIS), and Accreditation.

SY3 is a Royal Navy officer who began by expressing concern about the use to which his answers would be put. Following a short explanation the interviewee agreed to discuss security issues and raised some interesting points. The interviewee talked about the difficulty of ensuring that Users read and adhere to Security Operating (SyOps) instructions. Users circumvent the rules and the use of USB memory pen was cited as an example The rules state that only MODUK authorised (crypto enabled) data pens can be used with MODUK systems and that these data pens must not be used on any other system (e.g. private laptop). So, if a member of staff is under pressure to finish work, and this can only be done at home, then they will break this rule. Rules are also overridden in urgent operational circumstances. For example, to transfer information between international partners. Communications security processes are generally considered to be good, but even here Users have been known to break the rules. The interviewee did not consider training to be a problem. A technical concern raised, is the ability to get anti-virus and patches to units. MODUK policy does not allow certain types of file extensions to be used over the network. This means that patches have to be mailed to ships and so can be out of date before being applied. When talking about wider MODUK issues the interviewee expressed concern about the 'disconnect' between what the military security organisation needs and the commercial service provider delivers; specifically, the destruction of evidence when service providers' priority is to restore the service not maintain forensics. The interviewee also described how the MOD's Computer Emergency Response Team and Joint Security Coordination Centre organisations work to protect networks and

systems. The interviewee also described the responsibilities of the RN Warning, Alerting and Reporting Point (WARP). This organisation deals with Information Systems. Another organisation deals with compliance checking, and there are physical security teams. We briefly discussed the numbers of RN IT security incidents in 2007/2008 but the interviewee does not want the figures to be released to the public domain. The interviewee made the statement that 'We spend a lot of time and resources protecting our information'.

INT1 is RN intelligence officer with 25 years' experience in MODUK. At first this interviewee was concerned about her lack of specific security experience or expertise. However, once settled, the interviewee was able to give valuable 'User' insight into operational security. This interviewee made the point that, at sea, 'the operational imperative takes precedence '. In other words, trying to apply security practice and principles when the ship is sinking is not necessarily a good idea. The interviewee suggested that working jointly with other nations each with their own systems, standards and procedures 'can lead to bending of the rules'. When asked about protecting information the interviewee's view was that 'there can be a disconnect between a user's awareness and an expert's requirements'. This suggests that a user can break the security rules without being aware that this is happening. The interviewee cited the operational need for data transfer between systems against the risk of miss-use of devices such as data pens. An overall awareness of the situation is required to ensure effective protection of information. The interviewee was of the opinion that HMG has over reacted to the 2007/2008 information security breaches. On the subject of training, the interviewee again talked about the operational imperative. 'We are trained not to break the rules. But obeying the rules

and doing the job right takes time. Therefore there has to be value judgement'. The interviewee suggested that there is a need for the RN to improve its information culture. One of the interviewee's concerns was that 'growing expectations for IT are not always being met'. The interviewee also suggested that there should be plans in place when things go wrong. Rather than disconnect systems from networks new technology could allow security managers to execute a more surgical response to incidents. This interviewee was the only one to mention the Official Secrets Act 'In general, in the Services we deal, live and breathe security. We have the Official Secrets Act as the ultimate sanction'.

INT2 is a Royal Navy Intelligence Surveillance Target Acquisition and Reconnaissance (ISTAR) specialist with over twenty years' experience. The interviewee was pressed for time which resulted in a rushed interview and less depth (30 minutes). The interview started with a discussion about recent ICT events. He suggested that the migration to a new system, which took place in 2008,was a step back in capability. He was also concerned about the amount of time required just to manage e-mail on a daily basis. While discussing life at sea he pointed out the constraints due to bandwidth, limited space, and strenuous routines. There is also pressure on the availability of equipment. As an example he cited that 'juniors' have to queue to get on the system. However, the ability to 'fight the ship is well provisioned'. Returning to the issue of bandwidth, INT2 suggested that the lack of bandwidth leads to serious information deficiency. In INT2's opinion there is not an information overload, rather 'people pushing rubbish'.

ENG1 a Royal Navy engineer with 20 years' experience in ship systems management and project management. The interviewee appeared relaxed and willing to answer the

questions. In the interviewee's experience the maritime environment is more difficult to work in compared to a similar land-based environment. Technical issues cited included a lack of both bandwidth and communications connectivity. One effect is that ship staff still require paper documents to be kept up to date rather than rely on the electronic version held on the network in the UK. In the opinion of the interviewee support activity is not good and time is wasted reformatting information which is still of little value to Users. One of the difficulties identified by the interviewee is a lack of training. When asked about information assurance, the interviewee noted that there is a paradigm shift away from the 'need to know' towards a 'need to share'. In terms of continuity and recovery planning, the interviewee said that 'We [RN] have lost the knack. Information Assurance is ignored, not trained, not exercised'. Greater complexity of connections and poor working practice will worsen the situation. Whilst talking about joint operations with UK and international partners giving rise to opportunities for the ill-disposed, the interviewee reflected on the lack of general security training, security understanding and security control and cited an incident were a local Internet service provider was allowed to set up an Internet 'hotspot' on-board a ship. Also, the deficiencies in security awareness compel security 'crack downs' which in turn can stifle business activity. 'With a lack of understanding you cannot take risks.' Even so, the interviewee stated that in his opinion an electronic security attack on a ship would be relatively expensive – there are likely to be cheaper options for conducting attacks. When asked about security threats and vulnerabilities the interviewee cited commercial outsourcing and sharing commercial networks which, whilst reducing costs, do raise the vulnerability to attack. 'We can defend the data with crypto over such networks but we do not defend the service provider'.

ENG2 is an engineer and education officer with 16 years' sea going and shore based experience. Citing the example of submarines, the interviewee talked about the challenges of an independent maritime unit including intermittent connectivity and limited bandwidth . He believes that technology will become smarter and potentially lead to a reduction of the number of units to achieve the same effect. In his experience, there is a greater use of data transmission compared to several years ago. When discussing information, the interviewee expressed the opinion that RN information management is inefficient with too much none-targeted information. Information management organisation on-board is undergoing re-organisation ahead of the changes required by the Information Assurance Maturity Model which itself is HMG's response to the data loses of 2007/2008. (See, for descriptions of data losses, Burton (2008), Hanigan (2008) and CESG (2008b).) Returning to technology issues, the interviewee talked about the likely effects of the loss of legacy fall-back to signal traffic and an inability to conduct optimal maritime operations specifically in joint environment. He believes the impact will worsen as the dependence grows. The threats are not new but there is improved ability to carry out a network attack. It is worth an enemy investing in attack capability. The interviewee suggested that the MODUK does not have a map of IT architecture being deployed and this makes management and defence of the networks inefficient. When discussing systems failure the interviewee suggested that the RN does not plan for recovery in the same way that a civilian organisation would. Security training is not considered to be wrong. The interviewee believes that Users find that 'Carelessness is simpler [easier] than security'. Returning to the IAMM, the interviewee expressed the opinion that the data losses were due to carelessness and a lack of appreciation of how easy it is to lose large volumes of information from electronic media when compared with the same

physical volume being lost or stolen from an office. However, he did think there has been an element of overreaction. Finally, the interviewee expressed concern over: increasing burden on individuals; reliance on commercial services such as Airwaves; the possibility of 'Jamming'; single points of failure; and the limited number of satellites. In a land environment you have alternative data routing that are not available at sea. However, he pointed out that a ship has a certain security that land environments don't have.

ENG3 is a Royal Navy Weapons Electrical Officer with 14 years of experience. The interviewee highlighted the challenges of; long deployments and limited communications; business continuity; irregular working patterns; exercises present problems of endurance; and noise. He pointed out that the physical distribution of books and manuals are now gone. Information management was categorised as inconsistent and it frequently difficult to find a unique single source of truth. Also incoherent which leads to bad practice. This, in turn, leads to additional workload and 'mountains of data which is useless'. Interviewee recognised that the HMG review has led to tighter procedures for handling and carrying data. Security measures are enforced to stop data leaving secure areas. System failure leads can be devastating; takes time to get back into old ways of working; leads to User frustration, and the loss of key information for decision making. In a coalition there must be a balance between security and openness. Current risk based approach to systems can be erratic and can slow down the speed of progress. However, lip service to security measures runs the risk of completely corrupting the operation. He believes that 'we are the poor cousins in terms of bandwidth. Most information systems take little consideration of bandwidth'. He suggested that expectations are too high 'At home

you can expect broadband and more'. He went on to say that 'On-board ship there is a single input path, which is expensive, technically limited and so we are constrained'. The interviewee suggested that work should be carried out to improve bandwidth efficiency. When asked about the threats, the interviewee talked about the limited number of 'points of penetration' [physical boundary around the hull] and that the RN uses protection techniques such as radio encryption. In the opinion of the interviewee, security training is poor from both an information and systems view point.

ENG4, a Royal Navy officer with over 12 years' experience of engineering capability development and combat systems accreditation. This interviewee regards the maritime environment to be more secure in the sense of a mobile metal box. There are difficulties due to bandwidth and he cited for example issues such as virus updates, patch information and ensuring access to latest advice and policy. He expressed concern with shore-based support solutions and reach back. Ship staffs no longer want to wait to get into harbour for solutions to problems, and this has security implications. When discussing information as an asset to be protected, the interview suggested that information management and security issues are not fully thought through at sea. He cited for example that the procurement of computing and communications equipment does not match the needs and limitations of the maritime environment. He described how the expectation is to be constantly in touch and how it is easy to get lost in red tape as a result. The interviewee also expressed concern about the lack of understanding in applying the ways of working. He believes that there is a lack of training at the basic level. Effort is in hand but need to embed ways of working within the RN culture. He believes that the needs of information assurance and the needs for networked capability are causing problems. On the one hand there

is the need to reduce the level of data transfers. On the other hand, there are operations based on the need to share. He suggests that effective assured delivery is what is needed. On the subject of systems failure, the interviewee was of the opinion that there is an over reliance on IT to conduct some compulsory tasks with no fall-back and a lack of disaster recovery. He described the push to a single network and likened it to 'putting all the eggs in one basket'. The interviewee believes that there is a poor understanding of security requirements due to over complication and contradictory instructions. For example, removable media must be encrypted but the approved technology is not available. He suggested that there is pressure on people to circumvent the rules to achieve outputs. While discussing security threats, he described how systems are designed and then security is applied. He believes there needs to be a step change in information systems design.

CIS1 is a senior Civil Servant, working in information systems support. The interviewee asked why he had been selected to answer questions about security. Following a short discussion he accepted the logic and was willing to answer the questions openly. This interviewee highlighted the following key problem areas. He believes that there is an information overload and the lack of deployed technology to help. Not all RN is using the cultural and behavioural guidelines and protocols put in place to help. Also, web technology is emerging as a solution but not everyone is using it properly. Staff have inconsistent levels of experience when using ICT. For example, they are still using attachments rather than links to document stores. He suggested that staff do not appreciate collaborative working versus dissemination or publish to wider audience that is now possible using team sites. Finally, records management is poor due to inadequate software and poor culture. Whilst discussing

Information Assurance (IA) the interviewee suggested that HMG's initial reaction to the 2007/2008 security incidents was a 'knee jerk reaction'. The interviewee also suggested that IA should now be set on the same footing as diversity etc. otherwise there is a risk of loss of skills. Whilst discussing the likely impact of systems failure, the interviewee mentioned reputational damage to MODUK, RN and C4ISTAR and in extreme circumstances the impact on operations. A virus could lead to the loss of capability as demonstrated by the multiple Conficker incidents. Fall-back systems such as Military Messaging are available now but new infrastructure with limited resilience can be a single point of failure and can lead to IP hacking vulnerability. The interviewee expects experienced hackers will look to exploit vulnerabilities in terms of malware and executable code. A further issue is that more sophisticated IT will require extra skills and on-board support. The interviewee went on to describe how, in a self-contained environment (at sea), a ship can be disconnected from the network and still run. In the opinion of the interviewee, poor understanding and training is probably the major cause of security incidents. Another cause is staff under pressure to deliver and so having to circumvent the rules, 'Achieving output is more important than security'. The interviewee noted that the Commanding Officer on-board a ship is more empowered to take risk than a counterpart ashore.

CIS2 is a Royal Navy officer with over twenty years' experience in RN, Joint and NATO CIS and engineering. The interviewee described working at sea in a hostile environment in terms of both the enemy and also the elements. In his experience limited bandwidth presents constraints 'which are not frequently remembered by the wider community'. Technology is eroding the degree of independence which has been cherished by mariners. The temptation exists to 'micro-manage' from shore.

While talking about Information technology, the interviewee used terms such as 'decision superiority' and the dependence good information and information management. His response suggested that information overload is sometimes an issue. A benefit of the new technology is ability to 'spread local situational awareness and to contribute to the wider picture'. There is now a requirement for smarter information management and for the need for local specialists and cited the re-introduction of a naval intelligence capability as one example. In the interviewees' opinion, the technological barriers are falling, but the bandwidth limitations and costs of commercial service providers are causing problems. He returned to the idea that other Services taking part in joint operations assume ships have a continual presence and high bandwidth, which is not always the case, especially during operational silence periods. The interviewee suggested that the major barriers are cultural. He then talked about the balance between the benefits of sharing and the risks of inappropriate sharing or operational compromising of operational security. The interviewee described information management as 'incoherent and aspirational. 'There is a huge desire to do better' and 'there is a realisation that we could do a whole lot better'. While talking about protecting information, the interviewee mentioned the differences between physical security and 'cyber' security. He went on to say that 'The current 'flavour' of our protection regime is very much centred on recent, very public, breaches of personnel data'. He suggested that the 'need to know' is currently taking precedence over than the benefits of sharing. Security guidance for Service personnel is available in Joint Service Publication 440 (JSP 440) (Ministry of Defence UK, 2009) and other restricted documents. The interviewee noted that accreditation and risk management structures are also undergoing changes. The boundaries and responsibilities of risk owners, as networks proliferate,

need to be defined. He stated that 'We cannot get a crisp definition of what an information asset is'. Returning to the public data losses suggested that Information Commissioner had 'effectively put the MODUK on quarterly report'. He then went on to describe the changes that are coming into force, and the bench marks being used to monitor progress (Information Assurance Maturity Model). The interviewee suggested that too much effort had gone into the technical aspects of the Defence IT infrastructure. He suggested that more effort is now required to exploit the benefits of a common network across Defence. Another issue is that 'the boundary between operations and operations support is increasingly fuzzy'. In the opinion of the interviewee the common network does makes the RN 'a more attractive target and the potential for more significant impact if an adversary is successful'. However, the counter argument is that a common network allows the use of more effective protection and awareness of our networks health and the attacks to it. On-board expertise will need to be uplifted so that cyber battle damage and repair can be continuous, spontaneous and augmentation from shore. The interviewee stated that the majority of security incidents are caused by their own people. Training and awareness are undergoing overhauls. He talked about computer network defence and attack but not sure how to work this in because we did not go into any detail. He suggested that there is a need for 'better understanding of process and process ownership and therefore who is empowered to manage risk, decide what are your key assets to be protected and developing a proper risk management approach rather than an ad hoc one'. Legacy technology still in use is causing problems, for example the cost of the upkeep of obsolete equipment and unsupported software. From an ICT security perspective, being at sea is best 'By inference we might think that we are potentially at less threat because of the tenuous nature of our connectivity and our

lack of continual presence makes us less attractive to external attack. I think the internal vulnerabilities are just as acute and the impact is potentially more acutely felt through the lack of expertise on-board and the lack of the ability to rapidly ship in that expertise. Once again, the bandwidth constraints to remotely apply patches and reach back to the hub. Physical security is much improved - you have a tin box around you to protect and deter'.

CIS3 is a Royal Navy officer with over twenty years of CIS operations and management. The interviewee described how the technology available ashore is now more accessible on ships. He cited the example that in 1984 mariners would place high frequency (HF) radio telephone calls through operators and by 2004 dial direct, web browsing and satellite television were available in the right conditions. Access to the Internet helps in disaster relief. For example, readily available satellite pictures of earthquakes can be used to help understand a situation. Then, by using the Automatic Identification System (AIS), the positions of merchant ships can be pinpointed and by the use of Inmarsat telephones they can be directed to assist. One of the security issues is the misuse of the AIS. He suggested that commercial gain can be obtained from knowing where your competitors' ships are. He also suggested that certain commercial companies are directing Masters to turn off their AIS. AIS can also be used for good. For example, in 2005 a Royal Navy helicopter 'ditched' into the Gulf of Oman. AIS and INMARSAT were used to coordinate the rescue. The interviewee explained why information is so important to the RN. He went on to describe why information management is difficult, time consuming and expensive. The information assurance problem is being addressed following on from the HMG security initiative. He suggested that it will take a lot of time and effort to make

successful. On systems failure, he pondered the potential impacts. He suggested that at worst huge impact on UK and world economy. An EM pulse could lead to economic meltdown and he cited the likelihood that, without further funding, GPS satellites are due to 'fall out of the sky' in 2018. The interviewee talked about internal and external threats. He described how firewalls and other security measures are enforced shore-side. However, there have been examples where ships staff have upload virus using their own memory devices. There is a lack of understanding of doing this sort of thing. 'We are always playing catch up with technology. As Singh (1999) points out, it is difficult to play catch up because of the rate of change'.

CON1 is a civilian employed as a project manager and is a former Merchant Navy Radio Officer, keen to help and provided contacts with commercial organisations. Having experience in both the Merchant Navy and Royal Navy, the interviewee was able to describe the on-board working environment in some detail. The following points were captured: relatively small community; almost wholly work-focused with no recreation or other outlets; the physical environment can be challenging, the weather, sea states and cold; there are long working hours with disrupted sleep patterns; and the confined space and closed community can lead to tension. Personal issues can exist and you have to be flexible. The interviewee went on to describe how working practices have changed from virtual isolation from your organisation and infrastructure when not alongside to 24 hour contact almost anywhere in the world. 'This feeds the stress already caused by the environment'. The interviewee expressed concern for those working at sea today including incessant information requests, enquires etc. When discussing the 2007/2008 data losses the interviewee noted that whilst that loss was due to lax policy and procedure, the reaction has been

a massive overcompensation and is hampering business, 'The organisation as entity does not understand the value of information'. Systems failure would immediately stop current dynamic command and control capability. This would impact on any form of decision making. 'They would use different words in a commercial organisation but the effect is the same'. Education of people is probably one of the biggest causes of failure. This is not a new challenge. The current approach to IT security is not intuitive and not yet simple enough to make training etc. simple. Whilst discussing threats to the networked systems, the interviewee talked about how the scale and scope of threats will be the daunting factor. The interviewee was concerned with the possibility that the infrastructure was introducing a single point of failure. Because of physical displacement of platform to land the point of linkage becomes point of failure, and because maritime platform alternatives and diversity are limited. On the subject of risk management, the interviewee talked about the need to 'evolve a method of risk management that is not just the current method of risk aversion'. Complexity means the ill-disposed, or anyone who may wish to attack the MODUK, need to become more sophisticated.

CON2 is a civilian security consultant working on HMG's Information Assurance Maturity Model (IAMM). The interviewee talked about the challenges faced in delivering situational awareness or sharing information. He explained the difficulty defending your own and others information such as the 'Duty of care'. He went on to talk about difficulties maintaining communications links including atmospherics, propagation and bandwidth limitations. The interviewee then described how pressure on the system puts pressure on security principles 'it is difficult to bring security principles to bear at extreme distances'. In the opinion of the interviewee information

assurance should not be technology driven. He cited the idea that 'what do I need to do, what do I need to prosecute, how do I prosecute it and how can I do that keeping a high quality of IA to do it'. So what technical solutions are available for me to do that. When considering the progress being made towards effective security, the interviewee suggested that progress is being made. A common [MODUK] understanding of terminology remains a challenge. Indeed, the use of [MODUK] terminology is different to that used in government. He also expressed concern that there is a lack of understanding of how information can be used correctly and that training is required. The lack of understanding of the technology makes it difficult to understand security risks. When you lose the understanding of the integral linkages between security, management information, knowledge management and exploit information starts to break down. The interviewee believes that the initial reaction, to recent security incidents, was to stop data sharing, but data sharing/movement is now improving, 'MODUK losses of information are starting to drop off'. Moving onto risk management the interviewee stated that 'There is no money to go back to an entirely risk free world – and life isn't risk free'. When asked about the effect of cumulative risk taking he talked about data disaggregation, financial risk reaching critical and a growing realisation that risk should not be allowed to stack up. [It has been the author's experience that data disaggregation has defied solution for many years and could be a project in its own right. The subject sounds straight forward in principle]. On the subject of threat, the interviewee believes that a good maritime threat and vulnerability analysis has not been conducted. As a result, decisions are being made without the full facts.

CON3 is a civilian Information Assurance consultant. The interviewee suggested that it is better to have security technology that supports people rather than technology with all the 'bells and whistles'. He went onto to put forward the observation that bad security practice is a cause for incidents but also the need to get the job done leads to taking short cuts. If security practice is embedded in normal business then business practice should improve and management of risks become standard practice. Another point raised is the new linkage between career progression and disciplinary action such that the no blame culture is being replaced with facing the consequence of actions. This linkage is leading to improved behaviour on the part of users. The interviewee did not believe that accepting cumulative risk will have adverse consequences on ITSy in a maritime environment. He went on to explain that risk can be sensibly managed as long as mitigation processes are in place. Whilst discussing the IAMM he highlighted the effects of raising conscience, it identifies the frailties in explicate ways and helps to identify the investment strategy needed in order to improve. It would help if MODUK would adopt normal risk management processes in this area. However, MODUK is doing the right things; it just needs to get better. The security methodology and processes are good enough. The interviewee suggested that the maritime environment is a major driver on electronic and physical security threats. There is a need to apply the threat assessments and mitigation in the business context. There is a need to embed security design into capability design so that it enables rather than dampens and weakens practice. The interviewee observed that there is nothing worse than a bolted on security measure. The best way to achieve safety is by design from the first stage. He believes that ICT procurement across government should be based on design. [After the interview we talked about other MODUK initiatives, one of which is the three part MODUK Information Strategy

(MODIS). Previous versions of MODIS did not have a security component. The next version will].

A complete record of all the RN interview notes is supplied in column 2 of the table in Appendix B.

4.3 Data collected

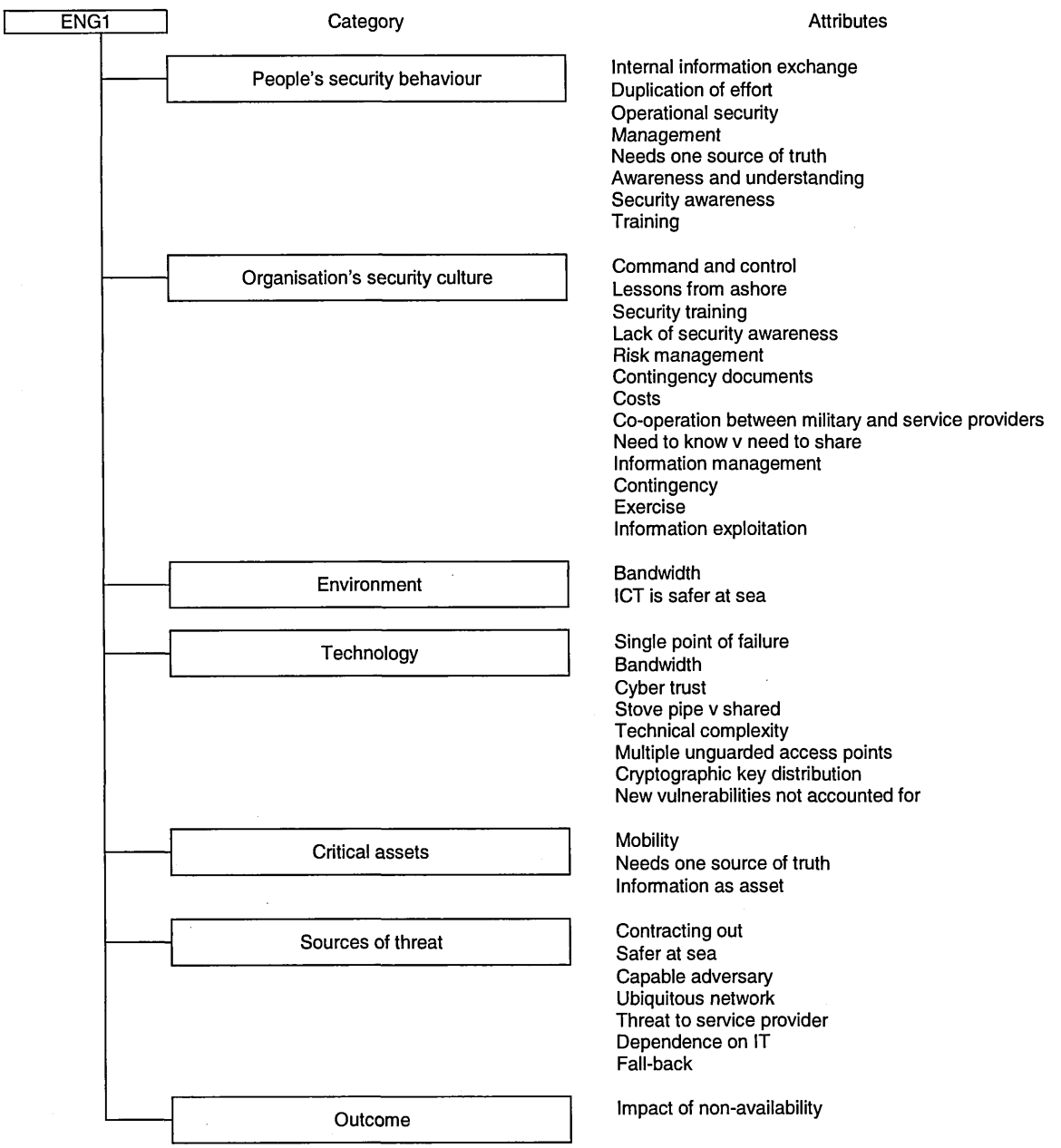
The RN notes and data were mapped into a table using an Excel™ spreadsheet for ease of data handling, as explained in Section 3.4. This spreadsheet was built with four columns. Certain of the interviewee's answers covered more than one topic. Where this happened the data have been separated into data blocks. The first column shows the mapping of the data block with its associated question from Table 3.4. The interviewee's opinions, as recorded at the time of the interviews, are mapped out in the second column. In this way, the data trail can be established (Yin, 2003), which in turn will help fellow researchers reflect on the original data, should they chose to conduct further research. The third column contains the results of the researcher's interpretation of the data using open coding and 'in-vivo concepts' (Corbin and Strauss, 2008, Kindle Locations 1017-1018). The fourth column records the research codes associated with barriers to ICT security. (See Section 3.2.) Data collected from ENG1 is provided here as an example. (See Table 4.2.)

Table 4.2: Extract of ENG1 data presented in four columns

Data block and question	Interviewee's opinions of ICT security in a maritime environment	Researcher's interpretation of interviewee's opinions	Research code
A Q1	Yes it does. You have the element of bandwidth which makes it more difficult. Other environments are similar: mobile environments. We have a paucity of communications connectivity.	1. Restrictions due to bandwidth 2. Similar restrictions apply in land environment 3. Limited communications options	181. Bandwidth 182. Mobility 183. Single point of failure
B Q2	We spend more time sitting on e-mail. Unfortunately systems are still stove piped. Organisation boundaries within single platform [chain of command] require communications using e-mail with little automation [no web working]. This means our on-board information exchange is poor. We still have to make sure our paper BRs are up to date and correct.	1. Intelligence, management, warfare etc. all on their own system 2. Self-imposed network restrictions 3. Duplication of effort (Paper and electronic books) 4. In case on-board systems fails	184. Stove pipe v shared 185. Command and control 186. Internal information exchange 187. Duplication of effort 188. Contingency documents
C Q3	Enormously. From a communications point of view [IT] is very important, but lots of underlying support activity is not done well.	1. Important for operations 2. Support activity	189. Operational security
D Q3	Operations stuff is weighed off [well done] but the support side absolutely terrible. For example, making reports and returns.	1. Reports and returns	190. Management
E Q3	How the information is held, including spread sheets; there is no compatibility and different formats. It is the same information but people busy reformatting. The information should be available – most tools are geared up to top level management. As such, the resultant information is no use to Users.	1. Time wasted reformatting to satisfy different parts of the same organisation	191. Needs one source of truth
F Q4	Haphazard, haphazard and haphazard; I refer back to my previous answer!	1. Haphazard 2. Haphazard 3. Haphazard	192. Information management 193. Information exploitation
G Q5	Information is an important asset, but it depends on which level of the organisation you talk about. At higher levels it is very important; lower down not cognisant of what information means. People are not trained	1. Information is an asset 2. Awareness of information as an asset varies across the organisation	194. Information as asset 195. Awareness
H Q6	There has been a bit of a shift. IA, in my view, completely focused on not getting it – the need to know. Showing signs of making sure getting it – the need to share. Poor on making sure information accurate and correct. Big factor of not managing it well.	1. Returned to an earlier paradigm, need to know, because of data losses 2. Starting to settle back into need to share 3. Issues with information management	196. Need to know v need to share 197. Information management
I Q7	As it stands from a support point of view and the way they operate or organised – if IT stops then everything stops. Ships don't sail, helicopters don't fly. IA processes should have allowed continuity – having the right fall-backs – but we have lost the knack. IA is ignored, not trained, not exercised.	1. IT critical for all operations 2. Lack of fall-back capability 3. Lack of contingency plans 4. Lack of IA awareness and understanding 5. Lack of training 6. RN does not practice for working without IT	198. Dependence on IT 199. Fall-back 200. Contingency 201. Awareness and understanding 202. Training 203. Exercise
J Q8	MT WAN etc. will give more access points and lead to more complexity. Difficult to co-ordinate encryption key handling. IP crypto may help. In a maritime environment [IP crypto] by 2012 perhaps further.	1. Greater complexity of connections and poor working practice will worsen the situation 2. Traditional cryptographic methods too expensive and complex for international network working	204. Technical complexity 205. Multiple unguarded access points 206. Key distribution
K Q8	Complete integration into DII. You cannot use it for what you need it for. New vulnerabilities to Centre. Single point of failure.	1. Ubiquitous network 2. Impact of non-availability 3. New vulnerabilities not accounted for 4. Single point of failure	207. Ubiquitous network 208. Impact of non-availability 209. New vulnerabilities not accounted for 210. Single point of failure

A summary of the categories and their attributes emerging from each interview was then built. An example is provided in Figure 4.1.

Figure 4.1: Example of data categories and attributes extracted from ENG1



4.4 Analysis: Preliminary barriers

Looking across the RN data's categories and their attributes yielded nine barriers. These were:

1. Tensions experienced between security experts and ICT users
2. Operational imperatives override security requirements
3. Security requirements impeding business process
4. A limited ability to recover from disruption
5. Unable or unwilling to share security incident information
6. Inadequate security training
7. Disruption to situational awareness
8. Unpredictable behaviour of people in difficult situations
9. A lack of ICT security awareness

These will be discussed in this sub section.

1. Tensions experienced between security experts and ICT users

ICT security requires formal structures and absolute compliance by users. Equally, users require flexibility and freedom to operate under the prevailing conditions and circumstances. This conflict leads to the first barrier which manifests itself as criticism of security processes by users. For example, citing security method which is too difficult to follow and security instructions that are not clear and often contradict one another:

> Don't make it too complicated or boring. The current approach to IT security is not intuitive; not yet simple enough to make training etc. simple.
>
> CON1J

Conversely, there is criticism of users by security experts who claim that the principles and processes are more than sufficient to provide security if they are implemented correctly:

> The RN and MODUK have the right security processes and practices in place.
>
> SY2L

However, the same security expert expressed the opinion that:

> The MODUK security manual is considered to be large and unwieldy by the community that use it.
>
> SY2L

Such tensions are not limited to security and operations. The ISPS Code points out that there care must be taken between balancing the requirements of physical security and those of health and safety.

2. Operational imperatives override security requirements

This barrier tends to manifest when users need to act with flexibility in extreme circumstances. For example:

> I recently headed a team working in six separate domains. Each domain represented one country with different technical standards and operating procedures. Ashore we follow the rules, but work afloat requires an ability to conduct risk management. If the IT is insufficient, for example different networks, unconnected standalones and the need to use private IT then that can lead to 'bending of the rules'.
>
> INT1A

Security experts argue that security is there to protect all, regardless of the prevailing conditions and circumstances. The Royal Navy have introduced 'Impact Tables' to access potential damage.

> A 'Protective Marking' is related to national security breach. The Impact Table expands this into the loss of capability.
>
> SY2I

The truth probably lies somewhere in between such that any security process has to be balanced against operational imperatives.

3. Security requirements impeding business process

This barrier is different to the previous barriers because of poor security process being built into operational systems such that need to know is taking precedence over the need to share. This is akin to 'fortress' mentality where it can be difficult if not impossible to do business if overly draconian security measures are in place.

4. A limited ability to recover from disruption.

This barrier is the one that is most readily voiced by experts and users. From a security perspective:

> Crews must be prepared for autonomous working; there is a need for ships to be able to work without links to UK or other commands.
>
> SY2D

The complexity of marine ICT is not helping the situation:

> Greater complexity of connections and poor working practice will worsen the situation.
>
> ENG1K

It is particularly important to be self-sufficient and to be able to recover from incidents because of the likely separation from immediate assistance:

> Could be catastrophic to the business which in a military context could lead to a loss of life in a business context could result in a company having to file for bankruptcy.
>
> SY1K

5. Unable or unwilling to share security incident information

This barrier typifies organisational barriers. It is not unreasonable for companies to want to protect their own vulnerabilities, and giving away details about how they have suffered would jeopardize their commercial well-being. Commercial intelligence could give competitors a vital advantage:

> Commercial gain can be obtained from knowing where your competitor's ships are. I understand that certain commercial companies are turning off their AIS. This is allowed in high threat areas.
>
> ENG2B

The act of sharing information is, in itself a barrier when the communication channel is not secure:

> Naval ships often call us up on VHF and ask us for details of our passage. This seems a bit silly; anyone could be listening!
>
> MN3

6. Inadequate security training

This barrier appears to have agreement across the interviewees with one exception:

> I do not think training is a problem.
>
> SY3F

More often, the view is held that:

> Training is a huge issue. We are trying to improve.
>
> ENG1L

Also:

> Security training is poor from both an information systems and information technology view point.
>
> ENG4L

A third engineer pointed to a lack of understanding:

> .... there have been examples where ship's staff have upload virus using their own memory devices. There is a lack of understanding and training which leads to this sort of thing.
>
> ENG2J

In addition:

> The lack of understanding of the technology makes it difficult to understand security risks.
>
> CON2G

Rapid changes to ICT can make previously provided training obsolete, and even with training in place, all's not well:

> With only a few hours training I have to read books to catch up.
>
> ENG4L

7. Disruption to situational awareness

This barrier has broad and profound consequences for those at sea. At its least disruptive, a loss of information can lead to inconvenience, perhaps a delay to a schedule or moving into an area of bad weather that could have been avoided had a weather forecast been received on-board. At its most disruptive, the loss of such information can lead to a severe incident with the potential to lead to a maritime disaster.

8. Unpredictable behaviour of people in difficult situations

This barrier represents a fascinating aspect of life at sea. One could use the indicator that information overload is causing stress:

> It was not long ago that when you sailed you disconnected from the organisation and infrastructure. In a period of 20 to 25 years that has radically changed. The rate of change has increased and network enabled ships leads to longer detached working. This all feeds the stress already caused by the environment. I think it must be horrendous to be at sea and being fed by the e-mail machine – information requests, enquires and demands.
>
> CON1B

However, this stress could be self-imposed:

> There is not an information overload, rather people pushing rubbish.
>
> INT2F

The main source of data for this barrier comes from secondary data and the way people behave in circumstances which they are not familiar with. For example, they may not be willing to carry out security duties in difficult circumstances (Self-

preservation). Remote monitoring and control from shore can lead to an even greater reduction of skills to deal with security issues on-board. There are psychological barriers caused by isolation from family and friends for extended periods. Inter personal issues can become a problem:

> It's a relatively small community. Focus almost holey work focused with no recreation or other outlets. The physical environment can be challenging, the weather, sea states and cold. There are the long working hours with disrupted sleep patterns. The confined space and closed community can lead to tension. Personal issues can exist and you have to be flexible.
>
> CON1A

9. A lack of ICT security awareness

This barrier has fundamental implications. It could be argued that this lack of awareness is due to an idiosyncrasy of the organisation. However, the need for a supposedly mature security organisation such as the RN to introduce the Information Assurance Maturity Model suggests otherwise:

> Information Assurance Maturity Model, which is HMG's response to the data loses in 2007/2008.
>
> ENG3D

The Information Assurance Maturity Model was introduced across UK government departments in an attempt to stem and then correct the loss of personal data and increase information security awareness across the National Health Service, the Ministry of Defence and other government departments and agencies (CESG, 2008b).

4.5 Analysis: Barriers and how they manifest themselves

A second pass was made through the RN data in an attempt to understand how barriers manifest themselves in the maritime environment. To achieve this

understanding, it was necessary to consider how the security, ICT and operations interact. Figure 4.2 shows a high level representation of the associated relationships.

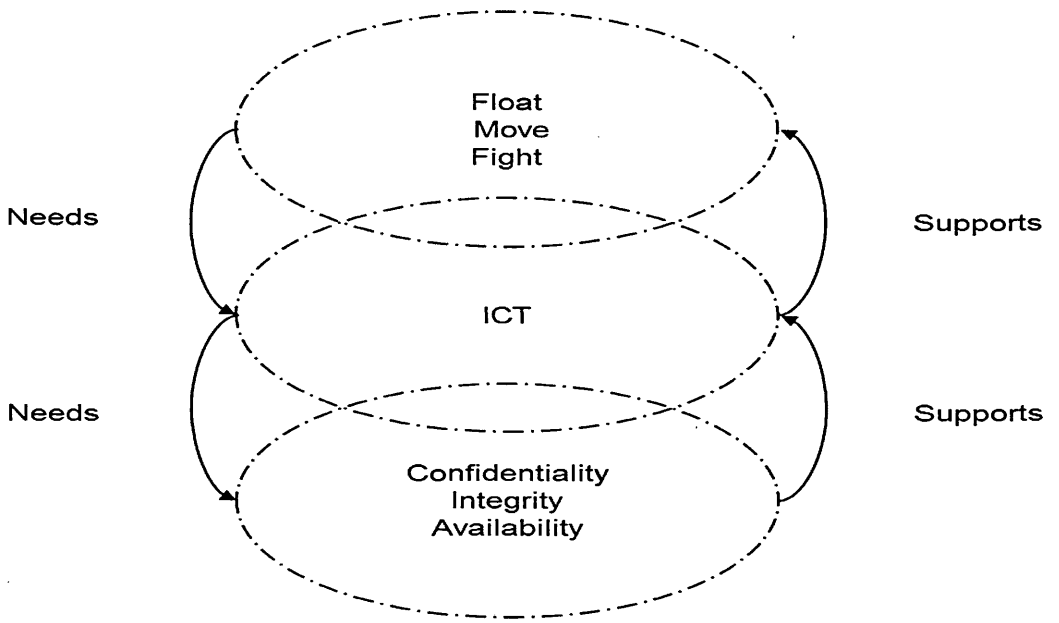


Figure 4.2: Interaction of operational, ICT and security components

In ideal conditions, the secure start state is such that confidentiality, integrity and availability (CIA) are functioning normally which in turn supports nominal ICT operations and the ability of the ship to float move and fight is at optimum efficiency from a secure ICT perspective. If a barrier to ICT security were to manifest then this in turn could have an adverse impact on the operational end state. In an extreme case, a barrier could stop normal ICT security functions which in turn could put the ship and her crew in danger. For example, if a navigational aid is taken out of service at a critical juncture. A barrier could complicate or confuse the security functions such that the operational end state is achieved but may not be fully trusted. Likewise, a barrier may slow a security function such that the end state is achieved but in this case it may be too late (*cf.* closing the barn door after the horse has bolted). A barrier may be present that causes concern in certain areas and yet is not recognised in others. In

this condition it is difficult to assess the effectiveness of security. A summary of these impacts is shown in Figure 4.3.

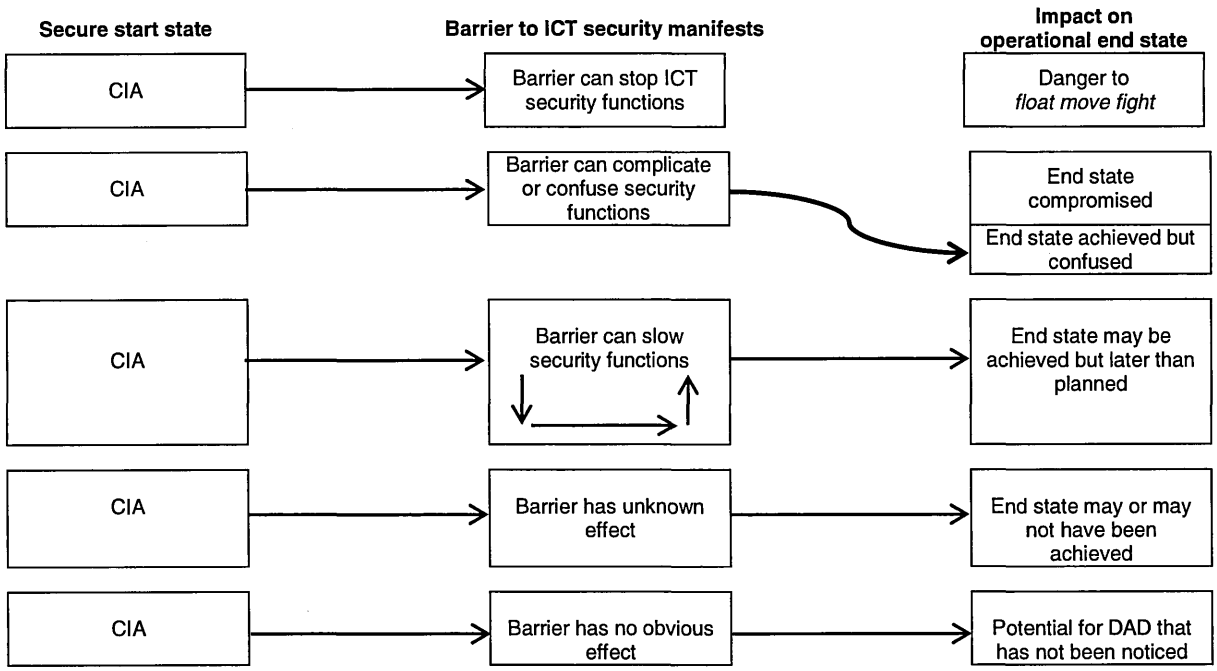


Figure 4.3: Barriers to secure ICT and how they manifest themselves

The impact can be further compounded because any given barrier can have multiple properties and dimensions and as such barriers can be conditional, or may not apply in all circumstances. For example, a security process itself can create uncertainty:

> Greater complexity of connections and poor working practice will worsen the situation.
>
> ENG1K

Such barriers may exist whilst the ship is alongside, but are greatly reduced when at sea and not connected to a radio network or vice versa. However, care must be taken to avoid complacency even when at sea and not connected to a network. For example, 'French Navy surrenders to Conficker' (The National Business Review, 2009) was an incident which started at sea on a standalone system and quickly spread when the system was connected ashore. This barrier category would be

manifest when users do not understand or are not even conscious of the need for ICT security. This incident was reported to have occurred in a Middle East port:

> ... to improve welfare connectivity a local Internet Service Provider (ISP) was used to set up a 'hot spot' on board a ship.
>
> ENG1M

In this case, no consideration was given to the security implications of having an unauthorised wireless transceiver on-board and the resulting potential for eaves-dropping, interference, and other security issues as described in Chapter 2.

Barriers can create significant obstacles to day to day operations and could have longer term consequences if business aspirations cannot be met or are interrupted in some way. A typical aspiration for ICT is:

> .... support not only the critical safety at sea, but will support the business drivers, certainly in the Merchant Service, which will be reducing operating costs whilst maximising profit.
>
> SY1A

Barriers of this type are those that could impede operations with the potential to initiate security breaches, and would likely be manifest when there are conflicts between the various departments, even a certain level of resentment. For example:

> During our last safety inspection we were criticised for padlocking hatches and doors. This went against our security inspection which required the same doors and hatches to be locked in some way.
>
> MN9

Barriers can be dangerous and this category is of particular interest especially in the context of Safety of Life at Sea (SOLAS), when a long way from immediate support in a potentially hostile environment. For example 'Limited ability to recover from disruption' would be dangerous if, due to the prevailing conditions and circumstances, mariners were unable to restore float move fight due to a lack of contingency capability. Barriers in this category will lead to incidents and disasters and will have to be alleviated as quickly and effectively as possible. One engineer suggested that a

loss of radio communications may not be an immediate issue but the loss of control of ship's systems could have an immediate impact:

> You can think of a big merchant ship losing communications may not be so serious – losing control of machinery mid Atlantic?
>
> ENG2

Another engineer stated that:

> If IT [ICT] stops then everything stops. Ships don't sail, helicopters don't fly.
>
> ENG1H

Should such a barrier lead to an incident or disaster at sea, then a self-contained, rapid response and recovery will be essential. For example, when HMS Nottingham grounded and subsequently lost main power, the battery powered GMDSS equipment was used to radio for help (Royal Navy, 2002). Individual stress factors are also characteristic of this this group of barriers:

> We end up doing this [security officer] and have no time for our day job.
>
> MN1

If a barrier is characterised as dangerous and is also attributed to an organisational shortfall, then this should be rectified or ameliorated. If, on the other, a barrier is characterised as inherent and is attributed to the laws of electromagnetic propagation, then the best that can be done is good design and an understanding of how to get the best from the prevailing conditions. This level of detail would be used by security experts rather than the users, and could help in the design, implementation and management of secure.

Barriers can be circumstance, location-dependant or inherent such that the owners and crew have little or no control and so would have to alleviate the impact if an ICT incident of this type were to take place. Of course, having a disaster recovery plan is essential, regardless of what caused the incident in the first place.

4.6 Conclusion

Analysis of the RN data, gathered between February and September 2009, has provided an insight into real world barriers to ICT security in the maritime environment. The first nine barriers that emerged from the data led to further consideration of the nature of barriers and how they manifest themselves. The results suggest that an understanding of barriers and their complex social and technical interactions could indeed be used to advance the understanding of security issues associated with the use of ICT systems in the maritime environment. It will therefore be appropriate to use them as a stimulus to develop a secure ICT maritime profile that will be capable of being updated on an on-going basis. This work will be further developed in Chapter 6 but before that the next chapter will present research undertaken to look at the Merchant Navy.

Chapter 5

Merchant Navy: Data and analysis

5.1 Introduction

This chapter looks at the Merchant Navy data gathered between June and September 2009. First, the data collected from opportunity based discussions with Merchant Navy officers will be presented. Then, a review of the structure of the ISPS Code Ship Security Assessment is undertaken to identify those components that are suitable for use within the proposed updateable maritime ICT security profile. Finally a review of maritime incident data from secondary sources will be used to reveal the potential threat actors and impacts that can be used to inform the updateable maritime ICT security profile that will be developed further in Chapter 6.

5.2 Data from the Merchant Ship Security Officer Course

In accordance with the methodology set out in Chapter 3, the data reported here was gathered on an opportunity basis during informal one to one conversations with Merchant Navy officers attending a Ship's Security Officer training course held in South Shields. During the course, there was no direct mention made of ICT security. However, certain aspects of on-board operations and physical security did arise which have implications for secure ICT. The key points to emerge from the conversations are set out below in the following order:

1 The attendees
2 Resource issues
3 Additional security technology requirements
4 Ship's ICT

5 Physical security
6 Safety verses security
7 Summary

1 The attendees

The course was delivered by an ex Master Mariner who made the point that the ISPS Code came into existence to help member nations strengthen their physical security processes on-board and in harbours, and as such does not cover secure ICT. The Merchant Navy officers attending were representative of a range of maritime sector activities including liquid natural gas (LNG) carriers, tanker management, bulk cargo carriers and the off-shore oil and gas industry. Permission to take notes and talk to individual was sought during the introduction session. There were no dissenters.

2 Resource issues

The first thing to emerge from discussions with officers was that there are resource issues where the need for additional crew to take on security responsibilities cannot be met because of budget constraints. Even where the ISPS Code calls for dedicated security staff, the work falls to existing crew members in addition to their principle role on-board. One officer summarised the situation thus:

> We end up doing this [Ship Security Officer] and have no time for the day job
>
> MN1

This is a sentiment which echoes those expressed by officers in interviews reported by Price (1972) about their life at sea in the 1930s:

> We are inundated with little jobs that we don't get paid for and this stops us from doing our real work
>
> Price, 1972, p. 11

Price (1969) noted that as result of the concerns from the 1930s, working practices across the maritime sector were updated to improve working conditions and reduce working hours. The impact of the introduction of new security practices suggests that, in this instance, lessons about best working practice have either been overlooked or set to one side.

3 Additional security technology requirements

The ISPS Code requires ship authorities to fit a 'Ship Security Alert System' (Lees and Williamson, 2009, p. 43) to their vessels for the purpose of sending a covert message to the ship authority in the event of an attack. Upon activation of the system, the relevant authority such as the ship's owners' can contact the military to ask for an armed intervention. If an armed response team is close enough, it can be dispatched and in position before the attackers can press home their attack or flee the situation.

The system is activated by a 'panic button'. Some ships have just one such button but others have a number distributed around the vessel. However, because the existence of the Ship Security Alert System is in the public domain (see, for example, Hesse and Charalambous, 2004) it could itself be targeted with the aim of disabling the security system before it can be activated. False alarms are also a problem:

> I set off an alarm once, because I did not know the 'panic button' was a pressure switch on the deck next to the chart table
>
> MN2

Clearly, if there were to be a large number of false alarms the impact of genuine alarms would be likely to diminish (*cf.* the boy who cried wolf).

In addition to problems resulting from malicious intent, communications security can also be breached inadvertently:

> Naval ships often call us up on VHF and ask us for details of our passage. To me this seems a bit silly; anyone could be listening!
>
> MN3

An officer described the help that merchant mariners receive from the UK Maritime Trade Organisation:

> I don't know who they are but we give them our position using e-mail and they give us information about where the pirates are
>
> MN4

The UK MTO was established in Dubai in October 2001 'to act as an interface between military and merchant naval services across the entire maritime industry and work closely with coalition forces' (Royal Navy, 2013). If the ICT is not available to provide this service, or indeed the information can be falsified, then merchant vessels could be lured into dangerous situations and denied help or support. (The Maritime Trade Information Centre was established in Portsmouth July 2013.)

4 Ship's ICT

The role of the Royal Navy was briefly discussed and typical of the comments made is this one:

> We do talk to them [Royal Navy crews] but I am not sure they know what we do or that we have to keep to tight schedules
>
> MN8

What happens if RN and MN have to work together and the communications and computer networks are not compatible or available?

There are occasions when ship's ICT is not 'state of the art' and although it cannot be confirmed by the researcher as the norm, one officer did comment that:

> We get the office's (Company HQ) old IT when they get their new computers
>
> MN6

5 Physical security

The course leader, drawing on his experience as a Master pointed to changes linked to ships security that have occurred over the years:

> My job was to keep my ship, my crew and my cargo safe. The last thing I would have wanted is barbed wire, locked citadels and armed guards. Times have changed
>
> CL1

He continued:

> Ships today carry more cash than they used to in my day – mainly to pay local chandlers and non UK crew
>
> CL1

It is not unreasonable to speculate that if companies have migrated away from paying crews and local chandlers with cash, towards an e-commerce or indeed e-banking way of working then the physical threat of theft may reduce but the virtual threat to ICT could increase.

Whilst discussing how physical security is provided, one officer stated that:

> We are not military people, we do not arm ourselves and we do not want to. Russian sailors are trained to military standards and they are quite happy to defend themselves
>
> MN5

HMG issued guidelines in 2011 which now allow British flagged ships to carry armed guards (HMG, 2011). Again, if the physical threat is effectively countered, then the virtual threat to ICT could increase.

6 Safety verses security

There are clashes between the requirements of safety and security. One officer stated that:

> During our last safety inspection we were criticised for padlocking hatches and doors. This went against our security inspection which required the same doors and hatches to be locked in some way
>
> MN7

7 Summary

Overall, the Merchant Navy perspective on security is interesting. There appears to be limited resources to carry out the requirements to counter pirate and terrorist activity, let alone any emergent ICT security requirements. Also, there are conflicts of interest between security, safety and day to day operations. The emergent requirements of secure ICT are not being addressed in a coherent way.

5.3 The ISPS Code: Function and structure

The ISPS Code is a physical security risk assessment tool that was instigated by the member nations of the IMO as a direct result of the attacks against United States in 2001 (International Maritime Organisation, 2004). In this section, its function and structure will be explored to identify those components that are suitable for use within the proposed updateable secure ICT maritime profile.

A ship security assessment has three principle elements. The first element deals with the need to identify 'existing security measures, procedures and operations' (International Maritime Organisation, 2003, p. 12). The second is concerned with the need to identify and evaluate 'key shipboard operations that it is important to protect' (p. 13). The third element is about establishing the order of importance of security measures by the 'identification of possible threats to the key shipboard operations and the likelihood of their occurrence' (p. 13). The final element is the need to identify 'weaknesses including human factors, infrastructure, policies and procedures' (p. 13) that will require addressing in the ship security plan.

The structure of the ISPS Code is not dissimilar to that of other security risk assessment methods such as CRAMM and OCTAVE (See Figure 2.1 and Figure 2.2). Put simply, both structures are in two parts. The first part details what need to be

done and second details how to do it. Therefore, it is intended to use the ISPS Code as the basic framework; whilst using OCTAVE to provide the necessary secure ICT terminology as shown in Table 5.1. It may be possible to re-use data gathered from the physical security assessment. Examples of the data gathered by the Ship's Security Officer are shown in Table 5.2.

Table 5.1: The proposed components and elements of an updateable maritime ICT security profile

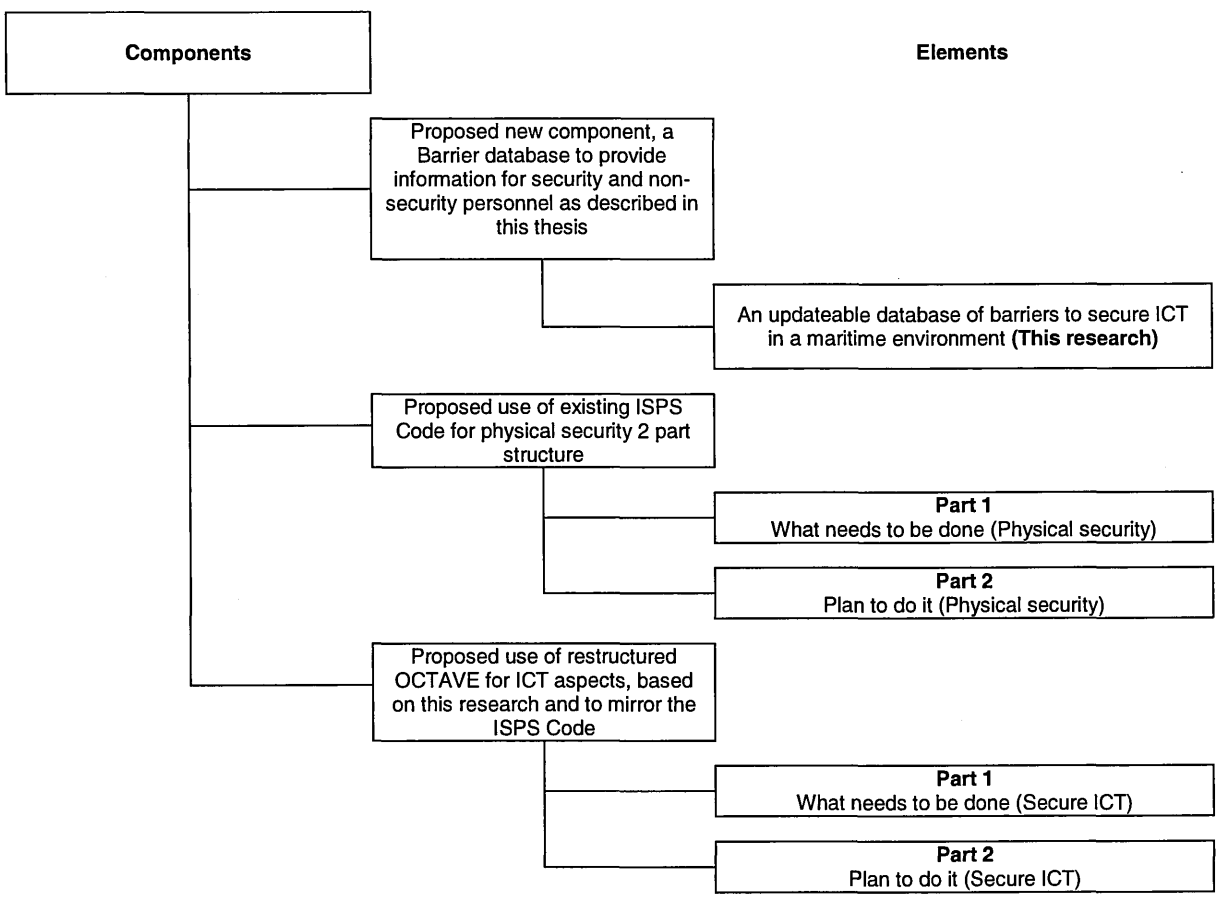


Table 5.2: Components of a Ship Security Plan which may inform an ICT Security Plan

ISPS Code, 2003, p. 57	Information in the ship's security assessment
Physical security	Identify restricted access ICT compartments and areas.
Structural integrity	Strength of access control to restricted access ICT compartments and areas.
Personnel protection systems	Identity cards and other security functions.
Procedural policies	Identifies the officers responsible for security
Radio and telecommunications systems, including computer systems and networks	The ISPS Code only mentions ICT. There are no internationally agreed provisions for ICT security procedures and processes.
Other areas	Boundaries between ICT and other areas. Can they be clearly delineated?
Existing security plans	What is already being done or is planned?
Critical assets, threats and vulnerabilities.	A starting point for the ICT security evaluation.

5.4 Potential ICT security incidents

Very little data exists regarding breaches of maritime ICT security but it is possible to shed light on the likely consequences of breaches by looking at failings that have resulted from other causes. The following general maritime incidents and activities have been identified as appropriate sources of information and are set out in this sub section under the following headings:

1. Criminal activity
2. Pirate activity
3. Terrorist activity
4. People acting under stress or duress
5. Mechanical and procedural failure
6. Inadequate training

These will now be looked at.

1. Criminal activity

Although the reported cases of deliberate targeting of secure maritime ICT systems are extremely rare, there is an increased potential to deliberate or accidental security incidents as recently confirmed by ENISA (2011) report on ICT security in the maritime sector. Most recently, an attack on the ICT systems of the port of Antwerp (Bateman, 2013) gives a portent of things to come. As Gill (1995) notes 'maritime crime has been a part of day to day life at sea for centuries' (p. 21). These activities range from insurance fraud and tax evasion to smuggling and theft of cargoes. Even though the understanding of these activities lies beyond the scope of this thesis, there is a growing likelihood that the people involved could attempt to exploit weaknesses in maritime ICT security. For example, if effective physical countermeasures weaken the links between terrorism and piracy then they may turn to cyber-attacks against marine ICT. Many of the issues related to piracy and terrorism lie beyond the scope of this thesis, but both activities are worthy of some consideration because of their current impact on merchant trade and the potential impact if they attempt to exploit ICT weaknesses.

2. Pirate activity

Whilst It has been suggested that there is little distinction between maritime pirates and terrorists operating at sea as both groups use similar tactics and therefore, as Chaturvedi (2010) argues 'both problems need to be tackled with a unified effort' (p. 24). However, Chaturvedi also points to the divergent motives of the two groups in that 'piracy is mostly undertaken for financial reasons, terrorism for political or religious reasons' (p. 24). Incidents of piracy on the high seas have increased in

violence and desperation (Lloyd's List, 2011). A review of the reports of pirate attacks reveals common operating practices including the use of small fast craft to intercept merchant and other vessels. (See, for example, the article entitled 'Applications and Shortcomings of the Law of the Sea in combating piracy: a South East Asian perspective', Collins & Hassan (2009).) There is also evidence to suggest that more sophisticated pirate operations use larger craft as support and supply vessels, and that even hijacked vessels have been used to act as an operating base. (See, for example, 'South Sea piracy, the Petro Ranger hijack', Economist (1999).) The pirates depend upon rapidly overpowering the relatively small crew complement on board merchant and other vessels.

As a countermeasure to piracy off the Somali coast, complex military technology is being pitted against desperate humans who have limited resources and nothing to lose (Jeory and Glannangell, 2011). Rothe and Collins (2011) argue that 'this military approach is like applying a sticking plaster to a major wound and avoids solving the underlying problems' (pp. 329-343). Glavovic and Boonzaier (2007) suggest that the main way of reducing piracy is to improve the livelihoods of coastal communities. For example, a One Earth Future Foundation study (Hurlburt, 2011) expresses concern over the impact on the Somali community where 'piracy affects food security and endangers Somali youth'. There is a strong temptation to attack shipping in areas where economic poverty is widespread (Pham, 2010). The opportunity to carry out attacks tend to occur where there is political instability and where vessels have restricted ability to manoeuvre (Hastings, 2009). Pham (2010) notes that 'piracy has always been a land-based crime which happens to manifest itself at sea' (p. 326) and

which suggests that any attempt to solve the problem will need to take a multi-dimensional approach which includes disrupting pirate's logistic bases ashore.

3. Terrorist activity

Although their motivations may be different, a review of the reports of attacks suggests that terrorist tactics at sea are comparable to those of pirates. For example, terrorist attacks off Indonesia have employed similar methods to the pirates off the Somali coast including the use of small fast craft and larger supply vessels in support roles (Banlaoi, 2005). However, political motivation can lead to alternative terrorist tactics as demonstrated on the 7th of October 1985, when four terrorists took control of the liner Achille Lauro[5] off the coast of Egypt and demanded the release of 50 Palestinians being held in Israeli prisons (Smith *et al.*, 1985).

Whereas pirates would likely prefer to stay out of the news, terrorists may welcome the headlines. The next two incidents have been classed as 'suicide attacks' giving an indication of the lengths certain terrorists will go to. It was reported that the American CIA worked with the Yemen security services to reveal intelligence[6] which linked the attacks on the Cole and the Limburg to the same terrorist group (Global Security, 2002). The Limburg incident was also significant because it was said to have been the first successful destructive strike at a sea going related target made by a terrorist group.

Destructive attacks against shore infrastructure can also be detrimental afloat even if no direct harm to mariners was intended. For example, on the 10th of April 1992 the original Baltic Exchange building was severely damaged in a terrorist attack which

[5] Also see, Italian fishing vessel 1971 and 2 passengers killed in fire alongside 1981 (Watson, 1995, p. 208)
[6] By intercepting mobile telephone and satellite telephone messages.

killed three people (Baltic Exchange, 2011). The activation of an ICT contingency plan allowed trade to resume quickly, first at Lloyd's of London and then in less damaged parts of the Baltic Exchange itself (*ib. id.*). However, it was the terrorist attacks in America on the 11th September 2001 which led directly to the implementation of the International Ship and Port Facility Security Code (International Maritime Organisation, 2003, p. 3). The ISPS Code deals with physical security threats and has no guidelines regarding the threats to maritime ICT; the International Maritime Organisation defers this responsibility to the International Telecommunications Union. Although the ISPS Code is a physical security risk assessment tool and guidelines for implementation of physical security, some of the data collected for a Ship Security Plan could be used to provide information for maritime ICT security profiles. For example, locations of ICT compartments, citadel arrangements, and emergency procedures.

4. People acting under stress or duress

The cruise ship Oceanos foundered off the west coast of South Africa on the 3rd August 1991 (ABC News, 1991). Whilst a Greek Board of Inquiry found the commanding officer, Yiannis Avranas, and four other officers negligent in their duties, the sinking was blamed on damage caused by heavy seas to one or more sea valves which quickly flooded an electrical generator compartment. Normally this compartment would have been considered watertight, and the flooding should have been contained. However, water entered other compartments via plumbing penetrations, so by-passing their water tight integrity[7]. What if this could be achieved remotely?

[7] HMS Nottingham also suffered the problem of: 'secondary flooding' via: 'compartment cable glands and ventilation penetrations' (Royal Navy, 2002, p. 8).

On 27 July 2005, 11 people died when a support vessel collided with the Mumbai High North production platform off the west coast of India (Baily, 2011). The resultant fire razed the production platform to sea level, destroyed a helicopter and the supply vessel itself foundered several days later. Rapid activation of the 'platform disaster management plan' averted a natural disaster when the sub-surface safety valves were promptly shut down. What if these valves could not have been shut down by a STUXNET type attack?

MV Herald of Free Enterprise provides another example of an incident caused by crew negligence and adverse commercial pressure (Sheen, 1987). Having sailed from Zeebruge on 6th of March 1987 the bow doors were left open, and during a turn to port, water entered the main car deck. The resultant free surface flood was not deep but was sufficient to cause the vessel to heel to port, eventually coming to rest on her port side in shallow water. 197 people died but 120 people, who had been trapped between decks, were eventually rescued (Watson, 1995). The jury in the subsequent coroner's inquest returned verdicts of unlawful killing (Records from BBC News Archive, 1987). However, Justice Turner directed the jury to acquit the company and several of the defendants. The inquest did set a precedent by confirming that the charge of corporate manslaughter is admissible in English courts, it was to take another 20 years before corporate manslaughter would become a criminal act in England (The Law Society, 2006). Herald of Free Enterprise was salvaged and sold for scrap in 1987 (Watson, 1995).

The next incident serves to highlight the adverse effect of commercial pressure, the impact of design change, crew stress and the cost to the environment when incidents are not well handled. Transporting hazardous cargoes by sea is a daily occurrence

and incidents involving such cargoes can have a damaging impact on the environment as demonstrated when the Liberian 'flagged'[8] crude oil tanker Torrey Canyon ran aground on Pollard's Rock off Cornwall's western coast during the early hours of the 18th of March 1967; all the crew were rescued by helicopters and lifeboats (Records from BBC News Archive, 1967). The subsequent Liberian investigation placed the entire blame for the grounding on a navigational error by Captain Pastrengo Rugiati, under pressure to meet a deadline, tried to take a short cut between Land's End and the Isles of Scilly (Nanda, 1967). However, it was likely that other factors were in play and Cahill (2002) reported that the structure of the Torrey Canyon had been altered such that the original design capacity of 60 000 tonnes was doubled to 120 000 tonnes following re-building in Japan, which led to the ship being under powered and slow to manoeuvre. Cahill also noted that a personal dispute between the Captain and the Chief Mate may have affected the Captain's judgement. An article in the Guardian (2011) has suggested that 'the incident itself was handled disastrously by British authorities at the time allowing the entire cargo to be released' and that 'the prevailing winds and weather caused 15% of the 119,328 tonnes of crude oil to hit the UK coast whilst most of the rest of the oil ended up on the Channel Islands and Brittany'. The adverse long term effect of such incidents was highlighted by the claim in the same Guardian article that 'the legacy of this disaster is still killing wildlife'.

5. Mechanical and procedural failure

The failure of equipment and operational procedures can come at a high human cost, especially when operating 8,000 miles from home and with limited logistical support. On the afternoon of the 4th of May 1982, whilst on patrol to the east of the Falkland

[8] Flagged – the country in which a vessel is registered.

Islands, HMS Sheffield (a Type 42 destroyer of the Royal Navy) was hit amid ships by an air to surface missile; the impact of the missile and the resultant fire and smoke killed 20 officers and ratings and injured a further 26 (Records from BBC News Archive, 1982). The BBC reported that 'within five hours the fires, dense black smoke and loss of essential services[9] forced Sheffield to be abandoned' (*Ib. id.*). Help was close at hand for the survivors nevertheless attempts to save the ship finally failed when, four days later, Sheffield foundered in deteriorating weather. A Royal Navy Board of Inquiry[10] revealed a complex set of events and a number of critical technical and human deficiencies which contributed to the loss of Sheffield (Royal Navy, 1982). On the face of it, a ship sinking as a consequence of military action has little relevance to a study looking at barriers to ICT security but one of the main findings of the investigation was that mutual interference between satellite communications equipment and electronic warfare equipment had led to the latter equipment being turned off throughout the period under investigation. This deprived the crew of situational awareness data at a critical time. It was also found that an important communications circuit was not manned during the lead up to the attack and this caused vital intelligence to be missed (*Ib. id.*). It is also worth noting that equipment and operational deficiencies were known about before the incident but the cost of correction was too high.

Incidents at sea are not confined to maritime mobile vessels[11]. On the 27th of March 1980 123 people from several nations lost their lives when a floating accommodation

---

[9] Firefighting capability, electrical supplies and communications.
[10] The Board assembled on the 7th June 1982 with the mandate to investigate both the situation leading up to and the conduct of the responses during and shortly after the incident. The investigation was conducted by serving officers of the Royal Navy.
[11] ITU description used to denote vessels of all descriptions as distinct from production and other structures that can be towed.

platform, the Alexander L. Kielland, capsized after one of the floatation legs sheared off in heavy seas; 89 people were rescued (Bignell and Fortune, 1984). Bignell and Fortune paint a vivid picture of the events leading up to the incident and in the immediate aftermath. They argue that the design, construction and operation of the platform had intrinsic flaws. For example, had the crew followed operational procedure when the floatation leg sheared off, then the watertight doors and hatches would have been closed and as a result the platform may not have capsized as quickly, potentially giving more time for additional survivors to escape. The investigation report noted problems both with the life raft communications equipment, and the 'on scene' incident co-ordination of the rescue effort; the incident commander changed several times and critical information about the situation was lost. The severe weather conditions also contributed to the poor co-ordination of the rescue effort. As the years have passed various conspiracy theories have arisen. For example, the accident is said to have been a deliberate act of sabotage in an attempt to stop Norway from exploiting North Sea gas and oil fields (Stavanger Museum, 2005). The possibility was raised that the ecological and human cost of gas and oil extraction in the North Sea was too high to continue and it would be interesting to speculate on the current economic situation in the UK had this line of reasoning been acted upon.

6. Inadequate training

The next incident highlights the consequences of shortfalls in seamanship training and poor situational awareness which led to the severe damage caused to a Royal Navy destroyer when, on the evening of the 3rd September 1988, whilst attempting a complicated manoeuvre in the dark, HMS Southampton collided with MV Torbay, a

container ship (Royal Navy, 1988). Southampton was badly damaged, with the starboard side of the bridge being crushed beyond habitability. No one was killed but several serious injuries were caused; the crew succeeded in keeping Southampton afloat and then steamed her to safe waters. The ensuing Board of Inquiry placed the blame for the collision on the negligence of certain senior officers and the lack of experience of junior bridge watch officers which led to the resultant 'failure to communicate intentions'. It was reported that the evidence given to the Board of Inquiry was often contradictory and lacking in detail which resulted in the Board of Inquiry recommending that 'a 'Black Box' recording system should be installed in all warships to help future investigations' and that 'investment should be made in a Bridge Simulator to improve training'. Both these recommendations were accepted by the Admiralty and the necessary investments made. The Royal Navy was without an important anti air asset for nearly two years and the cost of rebuilding was substantial because of the unique nature of the vessel. It is interesting to note that Members of the Board of Enquiry reported that they were denied access to MV Torbay for legal reasons.

5.5 Conclusions

Looking across the Merchant Navy data and the failings from other causes reveals that life at sea can be fraught with difficulties and that the ability to *float move fight* is of paramount importance to enable human activity in a maritime environment. ICT systems enable many aspects of life at sea and that there is a complex set of relationships between people, organisations, operations, environment and technical factors. ICT security is important everywhere but is difficult to achieve and maintain even in non-threatening environments. Life at sea has to be self-sufficient, robust and

able to recover from failure in exceptional circumstances if disasters are to be avoided. Mariners have a dependence on maritime systems of all types including emergency communications, engineering and logistics. The people using maritime ICT systems are under constant pressure, and in the face of incidents they can tend towards self-preservation rather than the needs of the many. There are complex national, international, organisational and legal issues. Insufficient training and awareness can lead to incidents. The previous scenarios when applied to maritime ICT security may appear far-fetched and with little supporting evidence. However, what if, for example, physical piracy becomes less lucrative or difficult to achieve? Will the threat actors turn to potential security vulnerabilities of remote ICT, or at least the threat of cyber-crime to extort money? It may be possible that the headline 'French Navy surrenders to Conficker worm' (The National Business Review, 2009) could become the 'norm' rather than the exception. It may be possible to combine an attack against shipping in strategic locations with a cyber-attack on critical shore infrastructure. For example, Singapore is said to be one of the busiest ports in the world with over 6000 people keeping 1000 ships moving 24 hours a day (Phang, 2008). The operation of the port relies on automated ICT including the port management, cargo handling and traffic control systems. Also, Singapore harbour authorities have invested in an extensive wireless (WiFi) network (Anjum, 2008). The physical environment is unforgiving and protecting critical ICT assets by identifying the barriers will be important.

Chapter 6

Barriers to ICT security in a maritime environment

6.1 Introduction

This research has confirmed that the increasing dependence on ICT adds an additional security dimension to the complexities of working at sea. This chapter will draw together the different threads in the preceding chapters to design and build an updateable maritime ICT security profile that will help mariners moderate the effects of such security complexities. This profile is intended as a standalone entity although there is also scope for its integration into the ISPS Code for use as part of a sector wide holistic security assessment tool.

6.2 Barriers as a stimulus to develop a secure ICT maritime profile

This research has revealed a complex set of ICT interactions on-board, in a notionally secure metal box safe from ICT threats and vulnerabilities. However, the situation changes markedly when improved radio connectivity and the ability of remote web working are added to the equation. In this situation, mariners have to deal with the competing requirements of the 'need to share' operational paradigm and the 'need to know' security paradigm. One example of barriers that characterise conflict is when business drivers override security whilst security attempts to control a range of operational behaviours. If future maritime ICT incidents do have similar aetiologies then it is possible that mariners will be able to share a common understanding of barriers to ICT security which is applicable afloat and ashore. This understanding will take account of human behaviour and will be cost effective if properly administered.

Barriers, and the early reporting of potential barriers, could be used as indicators of possible ICT security issues. HQs and other organisations could then alert the ship's crew to new developments using plain language rather than security terminology. Crews could then report their concerns back to the appropriate authority. This notion can be expanded by using barriers as a two way translation tool. Again, the barriers could be presented in plain language for the users to consider and a deeper explanation of the barrier could be made available for security experts.

Whilst the barriers emerging from the research data are representative of the diverse range of issues faced by mariners, they are also redolent of the socio-technical issues associated with the disasters described by authors such as Turner (1983), Bignell and Fortune (1984), Toft and Reynolds (1999) and Pidgeon (2010). Assembling barriers into barrier groups may yield new insights, as Toft and Reynolds (1999) attempted to achieve when looking for 'common learning patterns' (p. 35) from the analysis of the findings of public enquiries.

Barriers could be used to identify the need for security countermeasures. For example, this could be used to identify where one countermeasure may serve in the place of multiple countermeasures. If the interpretation of a barrier appears in multiple boxes, as shown in Table 6.1, then this could indicate that a common ancestry exists and that it may be possible to find a countermeasure that will be effective across a range of security activities.

Table 6.1: Barrier groups useful for security experts to identify common security countermeasures

	Dangerous barriers	Conditional barriers	Barriers causing significant obstacles or problems	Location dependant or inherent barriers
People	xxx		x	
Organisation		xx		
Environment	xx		xxxx	xx
Technology		xxx		

Barriers could inform decisions about the level of escalation required should the security situation change. For example, the ISPS Code has three security levels for escalating a ship's preparedness if intelligence is received regarding the possibility of a physical attack. These levels are:

- Level 1 – Normal (No intelligence or other indicators)
- Level 2 – Heightened (Attack likely) (Extra security patrols etc.)
- Level 3 – Exceptional (Imminent or underway) (Disconnect from network until all clear) (Emergency procedures initiated)

International Maritime Organisation, 2003, pp. 64-65

Barriers could also be used to help assess threat factors. For example, Information Security Standard 1 (CESG, 2009) lists the items which should be considered when deciding the issues that should be assessed based on the prevailing security conditions and circumstances. For example, by comparing the threat factors with maritime specific barriers, as shown in Table 6.2, it would be possible to inform the deliberation between a Ship Security Officer and members of the ship's crew

Table 6.2: Threat factors (Drawn from Information Security Standard 1, CESG, 2009, p. 12) mapped to maritime barriers

Threat factors (IS1 residual risk assessment)	**Maritime barrier**
1. Environment factor – the factors that will be exploited by groups of potential attackers.	Ship isolated at sea (Physical attack) High value target (Cyber blackmail)
2. Number of potential attackers. This number will change depending upon the location of the vessel. Likely to be higher when alongside and connected to landlines.	Internal attack population External attack population
3. Clearances of potential attackers.	Internal personnel not having the correct clearances. External attack groups will seek to discover passwords and other parameters needed to access the network.
4. Outcome/Impact level	Outcome = likelihood v impact (See Table 6.3)
5. Technical facilities. The means to carry out an attack	How good are the cyber criminals?
6. Technical opportunities.	Weaknesses in the system.
7.Publicity of the existence of the system or information.	It is assumed that the attack groups are aware of the existence of the target systems
8. Proactive monitoring	Intruder Detection Systems. Network management.
9. Quantity of data. How much data is stored in one location?	Value of data to 'float move fight (FMF)' and 'disclosure alteration destruction (DAD)'
10. Assurance of countermeasures. Common Criteria. Penetration testing.	Security technology can be rendered ineffective by a failure to differentiate among critical information assets, poorly designed operating procedures or lax attitudes towards security within an organisation.

Barriers could be assigned an outcome level based on impact and likelihood. For example, impact is the effect that an incident will have on the ship and her crew:

- Low – negligible impact on the organisation (Safety)
- Medium – considerable but existence not threatened (Urgency)
- High – existence threatened (Distress)

Lees and Williamson, 2009, p. 19

Likelihood of an incident can be classified thus:

- Low – practically never
- Medium – once a year
- High - once a week or more often

The Open University, 2008c, pp. 43-44

The barrier outcome level is then derived from the intersection of likelihood and impact as shown in Table 6.3. This outcome level would then indicate the barriers that should receive primacy when designing contingency plans.

Table 6.3: Outcome levels based on similar tables from the Open University (The Open University, 2008c) and OCTAVE (Alberts and Dorofee, 2003, p. 222)

Impact / Likelihood	Low	Medium	High
Low	Low outcome	Low outcome	Medium outcome
Medium	Low outcome	Medium outcome	High outcome
High	Medium outcome	High outcome	High outcome

6.3 Maritime ICT security profile: A design proposal

The five key design elements to emerge from the research, literature and secondary data are:

Part 1: The building blocks

Part 2: Ship's ICT asset assessment and risk evaluation

Part 3: ICT security strategy and management plan

Part 4: How to update the profile - Method and sources of information

Part 5: Input from non ICT security experts

Each of these will now be considered in turn.

Part 1: The building blocks

In order to illustrate how well the barriers revealed by this research will work to help mariners to identify problems with achieving ICT security, the foundations and building blocks for an ICT security profile have to be established. This research has identified two primary contenders for this purpose: the ISPS Code (International Maritime Organisation, 2003); and OCTAVE (Alberts and Dorofee, 2003).

From a ship's physical security perspective, there are two key parts to the ISPS Code, the ship security assessment (SSA) which articulates what needs to be done in terms of security, and the ship security plan (SSP) which defines how to carry out the security requirements. Although the ISPS Code deals with physical security, the foundations needed for an ICT security profile are implicit. Indeed, the ENISA (2011) research (introduced in Chapter 1) suggests that there is a need to add an ICT security component to existing regulatory frameworks if a sector wide holistic security solution is to be achieved. Figure 6.1 and Table 6.4 show the parts of the SSA and SSP relevant to ICT that are being proposed as the basic building blocks for an updateable maritime ICT security profile. It should be noted that the components of Figure 6.1 have been assembled from text descriptions in the ISPS Code; the Code itself has no diagrams.

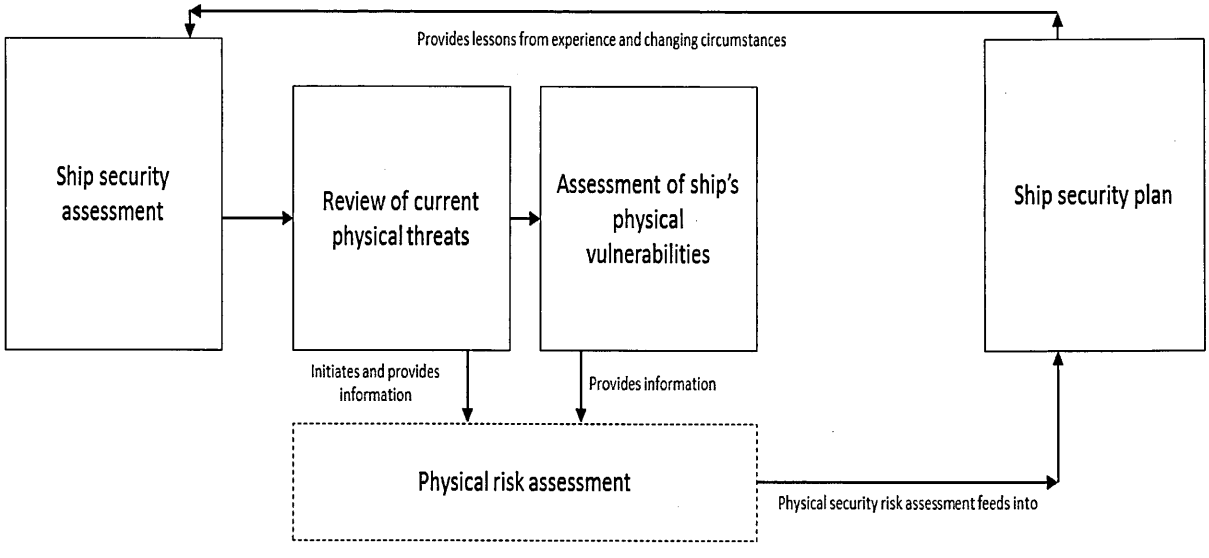


Figure 6.1: Basic building blocks drawn from an ISPS Code ship security assessment and ship security plan

Table 6.4: Description of components for physical risk assessment identified as relevant to an ICT security profile (IMO, 2003)

Ship security assessment (IMO, 2003, p.57):	Review of current physical threats (IMO, 2003, p.57):	Assessment of ship's physical vulnerabilities (IMO, 2003, p.60):
1. Detail the organisation structure of security for the ship	1. Knowledge of current security threats and patterns	1. Conflicts between safety and security measures
2. Detail the ship's relationship with the Company, port facilities, other ships and relevant authorities with security responsibilities	2. Recognition, on a non-discriminatory basis, of characteristics and behaviour patterns of persons who are likely to threaten security	2. Conflicts between shipboard duties and security assignments
3. Detail the communications within the ship and between other ships and port facilities	3. Techniques used to circumvent security measures	3. Watch-keeping duties, number of ship's personnel, particularly with implications on crew fatigue, alertness and performance
4. Level 1 operational and physical that will always be in place	4. Methods used to cause security incident	4. Any identified security training deficiencies
5. Allow level 2 to be quickly achieved and where necessary to level 3		5.Any security equipment and systems, including communication systems
6. Audit to respond to experience and changing circumstances		
7. Detailed reporting procedures		

Whilst the ISPS Code can offer the foundations for the ICT elements of an SSP, additional ICT-related building blocks are required to complete the proposed framework for the updateable maritime ICT security profile. It is proposed to draw on OCTAVE for this. OCTAVE is a 3 phase information security risk assessment process that has been selected to provide this function because of its operational bias, 'plug and play' structure and similarities to the processes in the ISPS Code. These characteristics allow the proposed ICT building blocks to be a mirror image of the structure of the ship security assessment and ship security plan, but using OCTAVE security threat, vulnerability and risk terminology in place of the physical security terminology. In this way, it is intended to have a format that security experts can readily appreciate. The associated OCTAVE risk template can be modified for a maritime-specific ICT risk assessment. The foundations and building blocks from the ISPS Code and OCTAVE are brought together in Figure 6.2 and the ICT risk evaluation template is given in Figure 6.3.

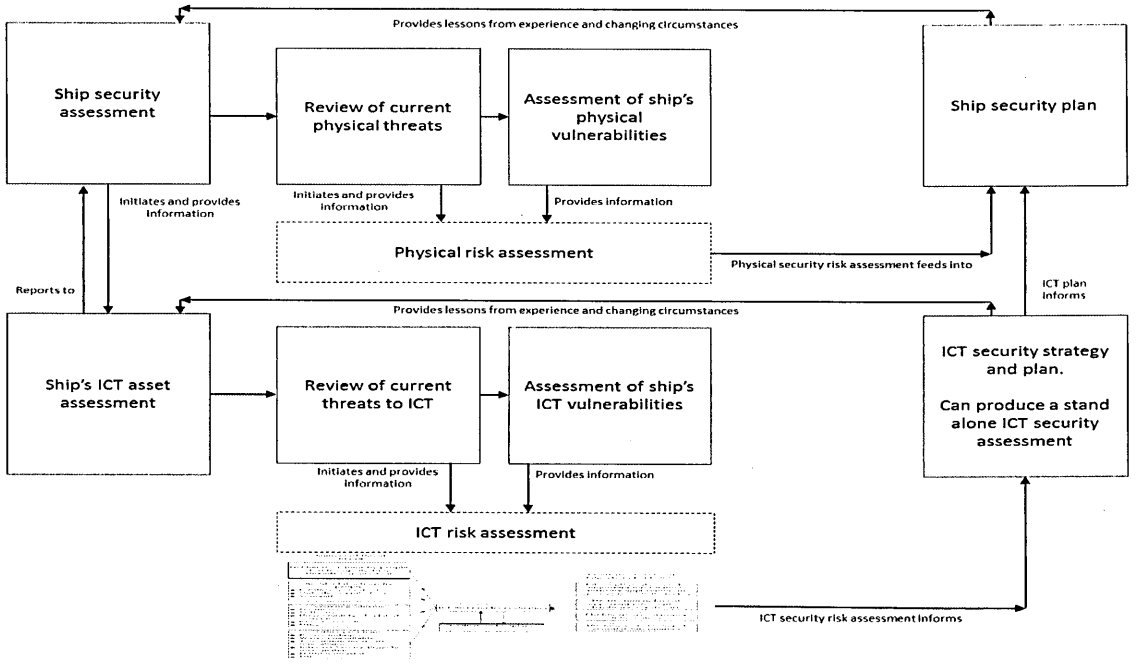


Figure 6.2: Fusion of ISPS Code and OCTAVE components, a framework for an updateable maritime ICT security profile.

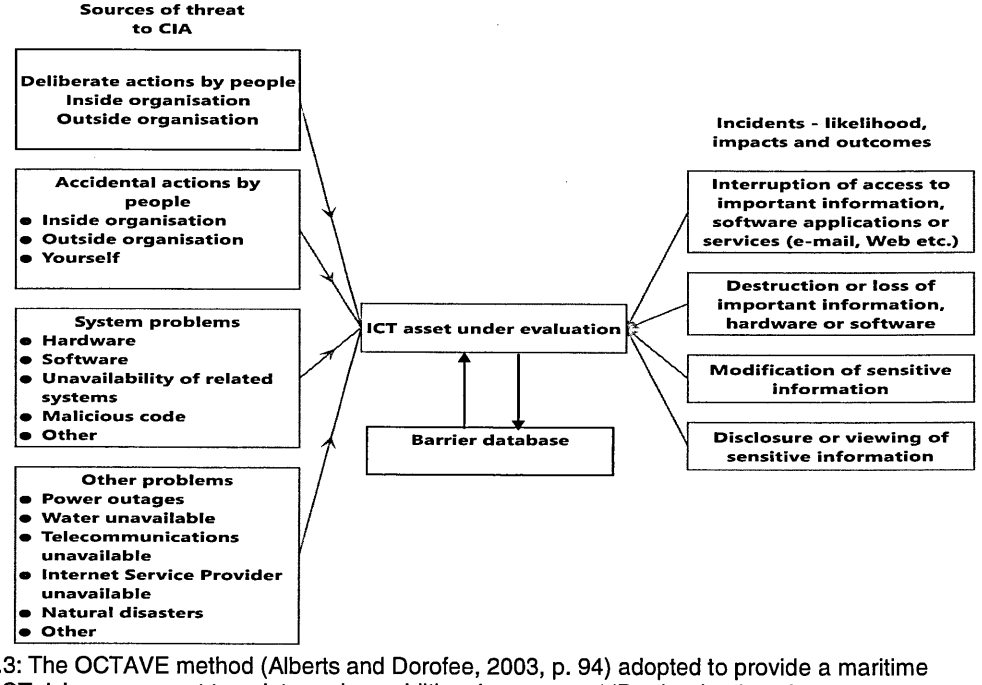


Figure 6.3: The OCTAVE method (Alberts and Dorofee, 2003, p. 94) adopted to provide a maritime specific ICT risk assessment template and an additional component 'Barrier database'

In order to use the asset assessment it is necessary to feed the results into a maritime specific ICT risk evaluation template. The assessment results would then be tabulated into an ICT risk profile. From this risk profile, security experts could create and implement an ICT security strategy and management plan that can be used as a standalone entity or to inform the ship security plan. The result of the fusion represents a traditional security model that will require a certain level of security training and expertise to complete evaluations successfully. An additional component will be required to bridge the perceived gap between security experts and mariners. Figure 6.4 shows this component feeding into the Ship security assessment, although it could also feed into the ICT risk assessment if the assessment were being used as a standalone entity.

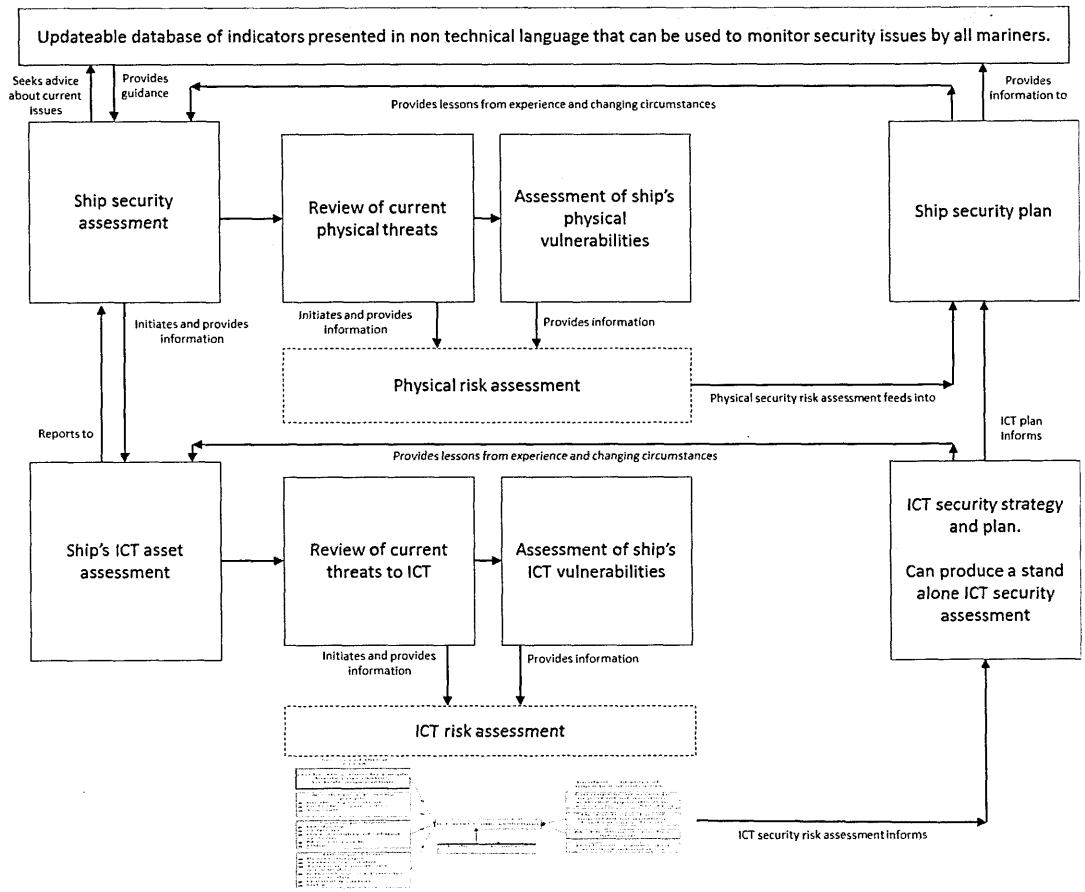


Figure 6.4: Updateable database with feeds to risk assessment and users

Part 2: Ship's ICT asset assessment and risk evaluation

The purpose of an ICT asset assessment is to identify ship-specific ICT assets in terms of their location, the associated wiring and power supplies, and the information required to run the ship. As this is the start of the assessment process, there will be potential for conflict between security, safety and operational barriers which evaluators need to be aware of including the following:

- Conflicts between boundaries of security and health & safety
- Conflicts between physical security and ICT security assessments
- Misunderstanding of local conditions

It is important to identify the location of all ICT assets and to this end three boundaries are required as provided in Figure 6.5.

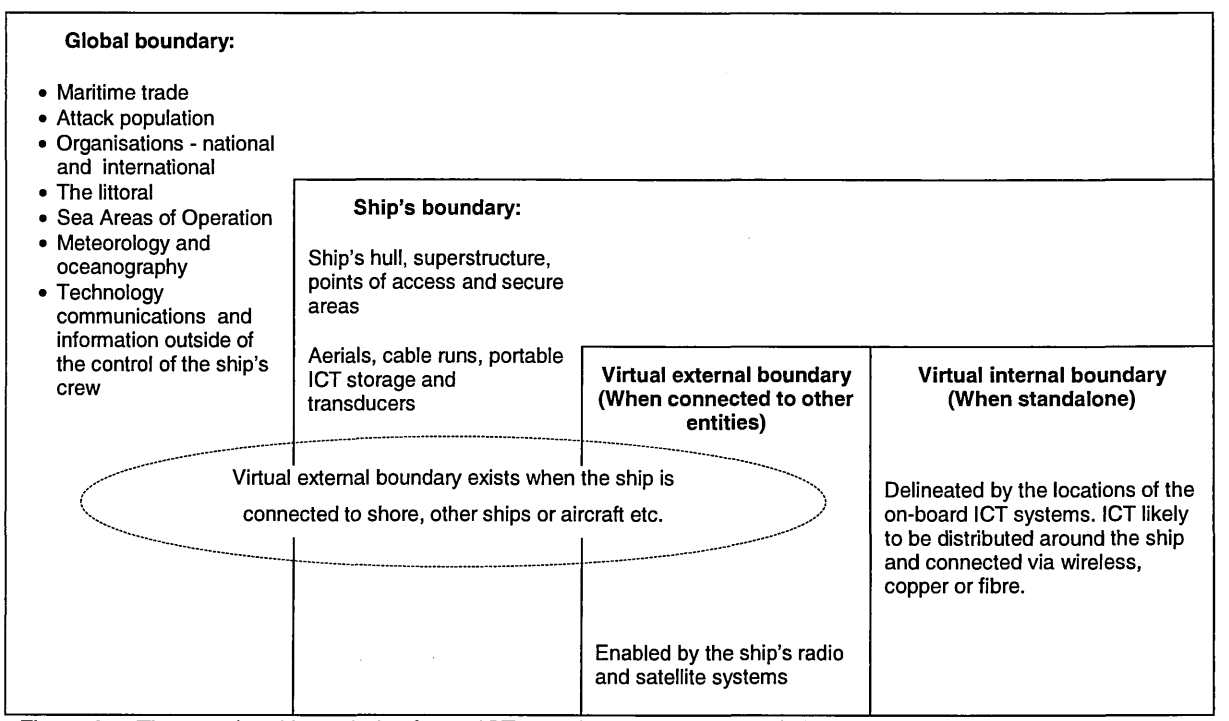


Figure 6.5: Three notional boundaries for an ICT security assessment, and showing networked ICT systems connecting across these boundaries

The first is the global boundary which encompasses those entities that can affect the ship or be affected by it. Such entities lie outside the control of the ship's crew, although attempts may be made to influence. Example barriers include:

- Interactions with organisations and the external attack population
- The littoral and Sea Areas of Operation
- Meteorology and oceanography
- Technology communications and information outside of the control of ship's crew

The second is the ship's physical boundary as defined in the ship's asset groups, provided in Table 6.5, and will include the hull, superstructure, access points and secure areas. The ICT asset assessment will provide ICT specific areas that are not covered by the ship's security assessment (for example, cable and aerial runs, aerials and other transducers and the locations of portable ICT including radios and other hand held devices). The third is the virtual boundary which has two distinct aspects. First, there is the virtual internal boundary that can be delineated by the locations of the on-board ICT systems (for example, computers, peripherals, sensors and data storage). Such ICT systems are located in areas, access to which can be readily controlled and are not connected to entities which lie outside of the control of the crew, such as the Internet. Second, there is the virtual external boundary which extends the virtual internal boundary when connections are made between entities using fixed land line (when alongside or at a buoy), marine radio or satellite links. Protecting the information that leaves the relatively safe confines of the virtual internal boundary requires more thought and greater effort. Figure 6.6 provides an illustration of the distribution of a ship's ICT and ICT supported or enabled functions.

Table 6.5: Ship asset groups, ICT and possible barriers		
Ship asset groups	Asset	Barrier
1. Ship's ICT	Aerials Cable runs Situational awareness equipment (Radar etc.) Distributed ICT SOLAS and GMDSS AIS and LRITS	Importance of fixtures and fittings not realised or accounted for Unable to operate if 'disclosure alteration or destruction of information occur Unable to call for help
2. ICT supports	Remote control Management Seamanship Engineering Logistics	Ability to float move fight' impaired
3. Ship's functional areas	Working spaces Citadel Limited access compartments Restricted access compartments Bridge, easy to identify on most types of ship. Secondary control positions	Conflict of interest between departments.
4. Crew performing operational functions	Seamanship Engineering Logistics	Lack of security awareness

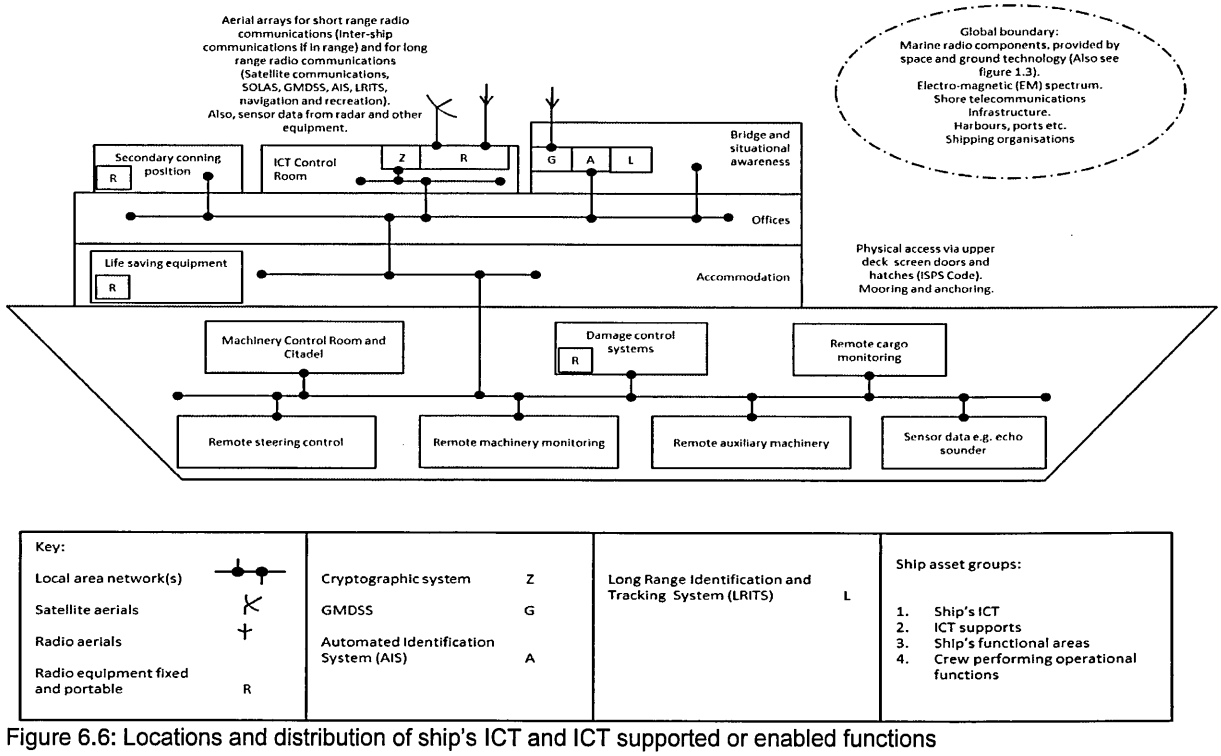


Figure 6.6: Locations and distribution of ship's ICT and ICT supported or enabled functions

The problems of risk evaluation run deeper than simple threat and vulnerability calculations. For example, Tullock and Lupton (2003) describe the understanding of risk as being challenging, not least because of the social and temporal dimensions involved:

> .... understandings about risk, and therefore the ways in which risk is dealt with and experienced in everyday life, are inevitably developed via membership of cultures and subcultures as well as through personal experience. Risk knowledges, therefore, are historical and local. What might be perceived to be 'risky' in one era at a certain local may no longer be viewed so in a later era, or in a different place. As a result, risk knowledges are constantly contested and are subject to disputes and debates over their nature, their control and whom is to blame for their creation.
>
> Tulloch and Lupton, 2003, p. 1

Risk must take account of everyday life, cultures, sub cultures and personal experience. Risk knowledge is historical and local and is constantly contested. For example, interconnection of systems has a cumulative effect over time:

> I am not sure whether businesses fully understand the individual risks they are carrying may have an impact on somebody else. At senior level, I am not sure they understand the cumulative effect.
>
> SY1Y

Risk may not be appreciated or arbitrary:

> I suspect risk taking is ill judged. We probably take risk we do not know about.
>
> SY2M

Several of the Royal Navy interviewees noted issues similar to that raised by SY1V:

> I see a greater need for security risk management. We security professionals could adopt the head in the sand approach: 'the answer is no, now what is the question?' The effect that has on business is potentially catastrophic. We need to be firmly embedded in business; we need to have a good understanding of business and the business needs to understand where we are coming from.
>
> SY1V

SY1V's statement contains a good example of security risk avoidance where security experts may try to avoid the issue by using delaying tactics:

> The answer is no, now what is the question?
>
> SY1V

Here lies a barrier between the traditional 'need to know' security paradigm versus the business oriented 'need to share':

> .... the current 'flavour' of our protection regime is very much centred on recent, very public, breaches of personnel data. Therefore, the pendulum has swung back towards the 'need to know' and a focus on protecting information and not sharing, rather than deriving the benefits of sharing.
>
> CIS1H

The literature contains many examples of social barriers including:

- Societal misperceptions of risk.

  Anderson and Moore, 2009, p. 2718
- Performance and productivity focus can on one hand lead to high risk strategies and subsequent adverse events. On the other hand over-regulation can have unintended consequences.

  Storey and Buchanan, 2007, p. 11

Returning to threats and vulnerabilities where virtual security can be breached at the speed of light:

> They (mariners) face the same threats and vulnerabilities and therefore the risk is the same perhaps just in different time scales.
>
> SY1L

Therefore, using the OCTAVE method will help to identify the generic sources of threat to confidentiality, integrity and availability:

- Internal (Deliberate) (accidental) (Crew and passengers)
- External (accidental/secondary effect) (Terrorist, pirate, others) (Deliberate)
- System problems
- Other problems

Drawn from Alberts and Dorofee, 2003, p. 94

The vulnerability assessment attempts to identify infrastructure weakness. It is anticipated that ships will have varying degrees of vulnerability depending upon their location and current state of radio connectivity. The overall result is an ICT risk profile for the ship, an example of which is provided in Table 6.6. This is turn informs the ICT plan for security countermeasures to support day to day operations.

Table 6.6: The result of a notional ship's ICT asset assessment and risk evaluation, mapped to the ship asset groups and the components under evaluation

Principle components under assessment	1. Ship's ICT	2. ICT supports	3. Ship's functional areas	4. Ship's functions directed, performed and monitored by:
	Aerials and sensors	Day to day operations	Superstructure	Master
	Radio communications	Electrical supply and distribution	Upper deck	Deck crew
	Local area network(s)	Propulsion	Hull	Engineering crew
	Server rooms	Damage control		Logistics crew
	Remote control and monitoring	Steering		
	Distributed ICT	Cargo management		
	Distress, Urgency and Safety	Situational awareness		
	Data storage and retrieval	Hotel services (Fresh water, sewage etc.)		

Part 3: ICT security strategy and management plan

The ICT asset assessment and risk evaluation from the previous section can be used to inform the ship security plan or can act as a standalone entity. There are two basic requirements for an ICT plan: security management to prevent disclosure, alteration and destruction (DAD: the consequences of a breach in CIA); and operational security to support float move fight. Relevant barriers drawn from across the literature and data include:

1. The lack of sustainable business models
2. Performance and productivity focus can on one hand lead to high risk strategies and subsequent adverse events. On the other hand over-regulation can have unintended consequences
3. Lack of managerial understanding and oversight of security
4. Failure of policies and procedures
5. Complex legal issues when trading crosses international borders.
6. Technical and business success relies on external partners.
7. How can an organization know if it is secure enough to detect and prevent security events that require business-continuity, crisis management, and disaster-recovery actions?
8. No effective bench marks to say if enough is being done.
9. Even achieving a certain level of security does not guarantee sustainability.
10. Delineating responsibilities when decisions are automated.

Security controls are normally put in place following the assessment stage are used to reduce any residual ICT security risk. Examples of security controls recommended by the Computer Emergency Response Team Co-ordination Center (CERT CC) are provided in Table 6.7. On-board, ICT security controls must be commensurate with the level of threat and the state of vulnerability at any given moment, for example during pilotage in restricted waters, the loss of situational awareness data could have a serious impact.

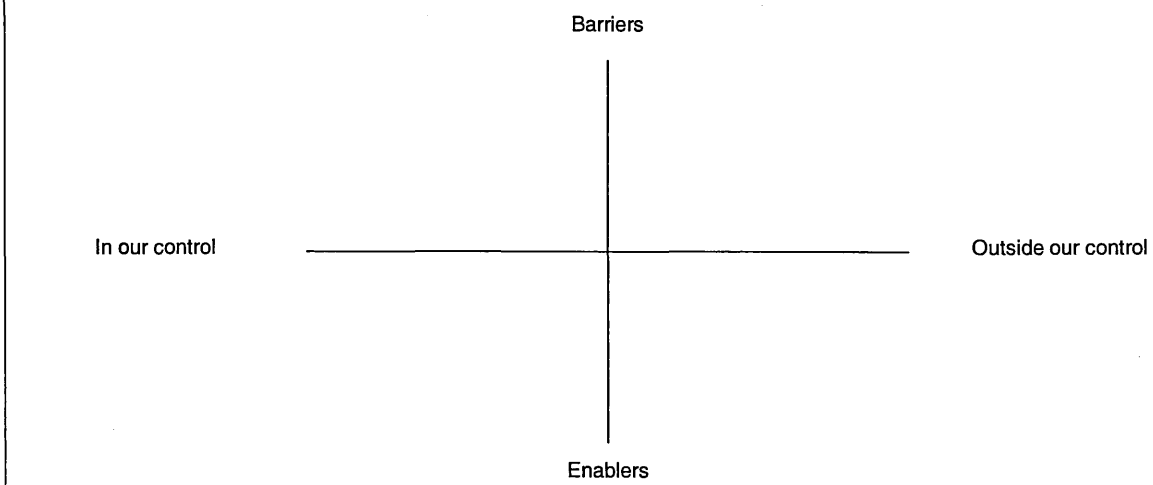
Table 6.7: Security controls that could be used in a ship ICT security plan and the barriers to watch for

Security controls version 4.0 (Carnegie Melon Institute, 2013)	Barriers
1. Inventory of authorised and unauthorised devices	Missing items Items not reported
2. Inventory of authorised and unauthorised software	Missing items Items not reported
3. Secure configurations for hardware and software on mobile devices, laptops, workstations, and servers	Complexity
4. Continuous vulnerability assessment and remediation	Time consuming Reasons not understood
5. Malware defences	Not updated False sense of security
6. Application software security	Not updated False sense of security
7. Wireless device control	Missing items Items not reported
8. Data recovery capability	Backups not taken Not stored correctly
9. Security skills assessment and appropriate training to fill gaps	Skills gap Lack of awareness
10. Secure configurations for network devices such as firewalls, routers, and switches	Complexity Technical skills
11. Limitation and control of network ports, protocols, and services	Technical skills
12. Controlled use of administrative privileges	Technical skills
13. Boundary defence	Boundaries not established Boundaries too fluid Responsibilities for boundaries not understood or in dispute
14. Maintenance, monitoring, and analysis of audit logs	Technical skills
15. Controlled access based on the need to know	Physical Virtual
16. Account monitoring and control	Local Networked
17. Data loss prevention	Security awareness
18. Incident response and management	Not available Not understood
19. Secure network engineering	Technical
20. Penetration tests and red team exercises	Too expensive Not understood

Part 4: How to update the profile - method and sources of information

Whilst it is important to learn from experience and changing circumstances, it is also important to be able to look forward in attempt to predicate and circumvent potential problems. Horizon Scanning is one method for monitoring future risk that has potential synergies with the findings of this research. The Horizon Scanning Centre (HSC) advocates use of the Backcasting method of Horizon Scanning to support the needs of divergent organisations that exist in complex milieus (Horizon Scanning Centre, 2013). Backcasting reviews a range of information from a variety of sources in an attempt to identify drivers and trends. The aim is to deliver solutions for problems that can appear to be intractable now or may not even be recognised as problems. For example, Table 6.8 provides an axial comparison using a 2x2 matrix that maps ICT security drivers and trends as either barriers or enablers and whether they are in or out of your control. Notwithstanding the choice of update method, from an organisational perspective, it is known that security updates and information for the ship security assessment and ship security plan will come from conventional sources such as the International Maritime Organisation, international and national communities and commercial security providers. Figure 6.7 provides the final version of the updateable maritime ICT security profile showing potential sources of barrier information and reporting.

Table 6.8: The use of Backcasting in a maritime environment (Horizon Scanning Centre, 2013)



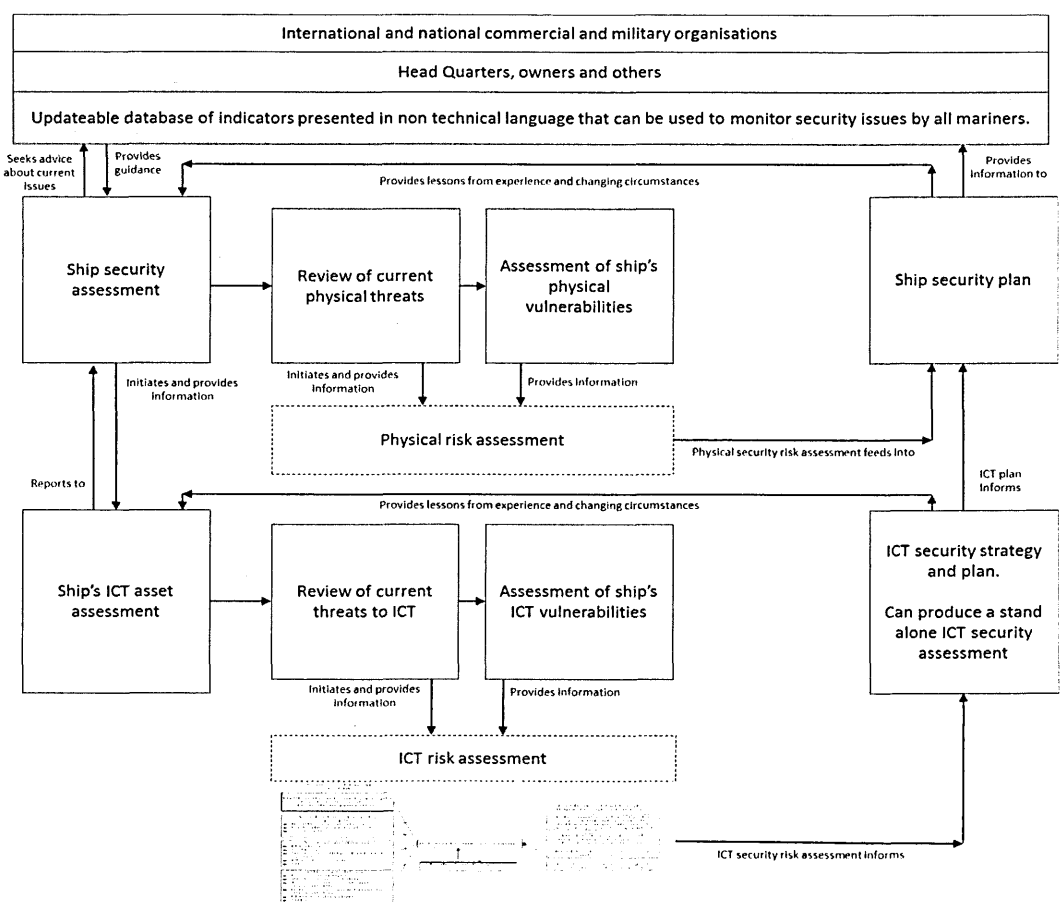


Figure 6.7: The updateable maritime ICT security profile with sources of barrier information and reporting

Whilst ICT security updates could also come from conventional sources, It is proposed that updates for the profile could come from international Maritime Trade Organisations. The UK maintains several MTOs including the Gulf and other locations. (Current operational deployments can be found in Royal Navy (2013).) A recent change to the structure came with the introduction of the Maritime Trade Information Centre (MTIC) which was established in 2013 to fill 'information management gaps' in the RN's security support to the Merchant Navy.

Part 5: Input from non ICT security experts

The ISPS Code and OCTAVE are designed for use where there are continuous reviews of security by experts from the physical and ICT security disciplines respectively. The research reported here suggests that if the secure ICT maritime profile is to be effective, then non-security experts will need to be involved in the process. It is proposed that the barriers themselves can be put to work, or more accurately, use the mariner's understanding of barriers to allow them to take part in the security assessment and monitoring processes. The rationale behind this thinking lies in the dual approach of using security experts based ashore to establish the safe physical and ICT working conditions and then engaging users at sea to monitor security. Those at sea would not be concerned with technical security issues *per se*, but identifying potential barriers that are relevant to ICT security which they can describe and are willing and able to report. In this way, the database can act as a two way translational tool that offers a realistic approach to the long standing issues identified in this research. The ultimate aim would be to have a web based updateable database of barriers presented in non-technical language that can be

used by mariners to monitor security issues. This topic is carried forward to Chapter 7.

6.4 Conclusion

If a barrier to ICT security exists or is created then it can lead to a threat, and that threat can be realised if an associated vulnerability can be exploited. Some of the barriers are straightforward and easy to identify and understand but others are complex and potentially have impacts at the strategic, operational or tactical levels of shipping functions that can have unforeseen outcomes. This chapter has drawn together the different threads in the preceding chapters to design and build an updateable maritime ICT security profile that that will help mariners moderate the effects of barriers to ICT security. It is proposed that the principles of Horizon Scanning could be used as a technique to keep the profile up to date. Chapter 7 will set out the final conclusions of this research.

Chapter 7

Conclusions

This chapter begins with a summary of the thesis. Then, an appraisal of the research questions is provided. Next, the contribution to the literature and suggestions regarding how others can use this work are outlined. At the end of this chapter, the strengths and weaknesses of the research methodology and recommendations for further research are provided.

7.1 Summary of this thesis

The research roadmap, first provided in Figure 1.3, is reproduced as Figure 7.1 with the addition of the chapters of this thesis mapped to the relevant sections. Chapter 1 established the context for this research by describing a worldwide mobile workforce that is coming to terms with the changing demands of ICT in a physical environment that is often hostile. The key innovations in maritime ICT, the dangers involved with being at sea and the need to call for help, were looked at. This led to the aim of the research presented in this thesis: to advance understanding of security issues associated with the use of ICT systems in a maritime environment. Specifically, the research sought to reveal barriers to secure ICT and use them to inform the development of a secure ICT maritime profile that will be capable of being updated on an on-going basis.

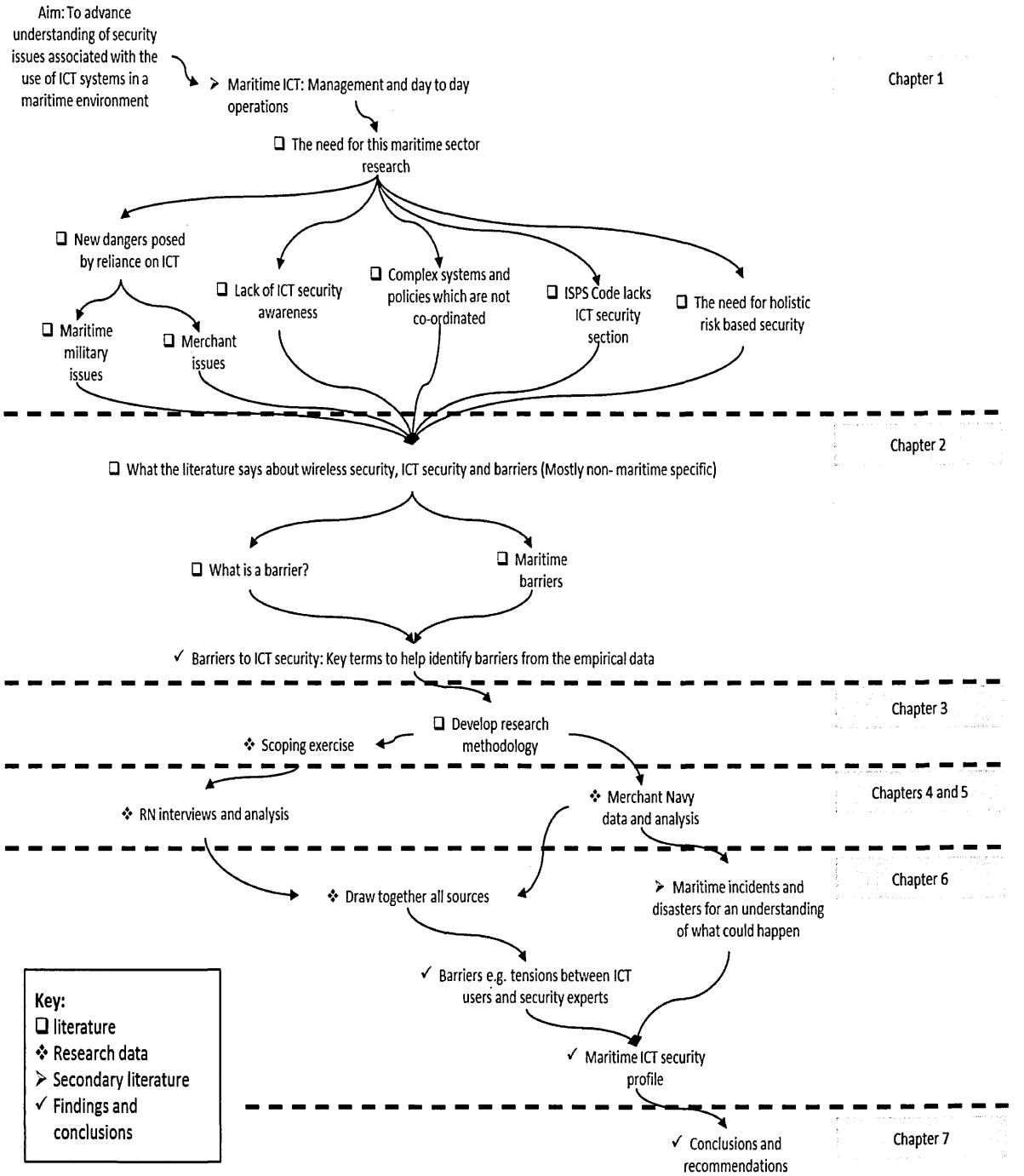


Figure 7.1: Research roadmap from Figure 1.3 with chapters mapped to the relevant sections

In the absence of literature that is specific to the maritime sector, Chapter 2 looked at the security characteristics of land based ICT which has the greatest relevance to the

maritime sector. This included wireless and cyber security. The literature was also used to define the nature of barriers and to identify the terminology associated with barriers to secure ICT. The resultant broad list of barriers as set out in Table 2.3 helped to identify barriers from the empirical data. Also, the results of this literature review enabled the four research questions to be formulated.

The research methodology, reported in Chapter 3, provided a satisfactory means to build on the literature reported in Chapters 1 and 2 which led to the development of an in depth view of 'real world' barriers to secure ICT that is presented in later chapters. This depth was achieved in the main by one to one semi-structured interviews with Royal Navy and Merchant Navy personnel.

The results of interviews with Royal Navy personnel were summarised and analysed in Chapter 4. The findings include a list of barriers and descriptions of security characteristics that could be used as examples of threats, outcomes and critical assets for use in the updateable secure ICT maritime profile. For a long time the data resisted deep understanding. The breakthrough came when the author returned to first principles and considered again the question of what is a barrier? This reappraisal led to the realisation that any given barrier can have multiple properties and dimensions. This in turn led to the identification of the correlation between objective barriers and security threats, and subjective barriers and vulnerabilities. An objective barrier is taken to be one that can apply in equal measure to all, and a subjective barrier is taken to be one that is perceived by an individual. In this sense an objective barrier is not unlike a security threat potentially faced by all whilst a subjective barrier is not unlike one that is perceived by an individual. Now, rather than the data being flat in the sense that it was not revealing anything new to the author,

the data came alive with information. In total, nine barriers were identified. (See Section 4.4.)

Chapter 5 reports the data collected from opportunity-based discussions with Merchant Navy officers. The parallel activity of reviewing the structure of the ISPS Code Ship Security Assessment successfully identified appropriate security components for use in an updateable maritime ICT security profile. Secondary literature was used to identify activities, such as terrorism and pirates, and incidents, such as groundings and collisions, to reveal the potential threat actors and impacts should an incident caused by failure of ICT security occur at sea.

Chapter 6 returned to the discussion regarding barriers and described how they acted as a stimulus for developing the maritime ICT security profile. The profile itself was developed in five parts by drawing together the different threads from the preceding chapters. The design and build of the profile is based on known security principles to help mariners moderate the effects of ICT security complexities. This profile is intended as a standalone entity although there is also scope for its integration into the ISPS Code for use as part of a sector wide holistic security assessment tool.

7.2 Appraisal of the research questions

The research questions were formulated in Section 2.7 and are restated here:

1. How are mariners responding to the increasing use of ICT and how and to what extent is their security behaviour adapting to the changes in technology?

2. What has been the impact of ICT on maritime organisations' security culture?

3. How have maritime authorities and organisations responded to the potential threats and vulnerabilities of maritime ICT?

4. Can the barriers be used as the basis for a secure ICT profile that can be used successfully in a maritime environment?

Each of these questions will now be discussed in turn.

1. How are mariners responding to the increasing use of ICT and how and to what extent is their security behaviour adapting to the changes in technology?

The research suggests that mariners are coming to terms with the increasing use of ICT but it also indicates are that they may not be adapting their security behaviour to the changing conditions and circumstances. Data to support these conclusions was presented in Chapters 1, 2, 4 and 5. For example, Chapter 1 provides a description of how maritime ICT has evolved from the late 1800s to 2013 showing that mariners were in the vanguard of adoption of radio and other technology and continue to make best use of technology. ICT security in a maritime environment is essential because of the growing dependence that mariners have on ICT. This includes emergency and commercial communications, situational awareness, seamanship, engineering and logistics. As such, working and living at sea calls for a level of self-sufficiency which is robust and able to recover from failure in exceptional circumstances if disasters are to be avoided.

2. What has been the impact of ICT on maritime organisations' security culture?

An attack targeting ICT could, at best, reduce the ability of mariners to be self-sufficient, or at worst lead to disaster at sea. The people using maritime ICT are under constant pressure, and in the face of incidents they can tend towards self-preservation rather than the needs of the many. There are complex national, international, organisational and legal issues which have to be dealt with as vessels cross jurisdictions. Insufficient training and awareness can lead to incidents that have

greater impact than they would elsewhere because the physical environment is unforgiving.

3. How have maritime authorities and organisations responded to the potential threats and vulnerabilities of maritime ICT?

With the exception of the ENISA (2011) report, little evidence could be found to suggest that any co-ordinated response to the potential threats and vulnerabilities of maritime ICT is in hand. Evidence from multiple sources suggests that it is difficult and costly for authorities and organisations to prepare for responses to threats without strong evidence to support the need such actions. Even maritime organisations that have a strong security culture built into their day to day working are struggling with the rapid changes brought about by new developments in ICT.

4. Can barriers to ICT security be used as the basis for a secure ICT profile that can be used successfully in a maritime environment?

The data and literature used in this thesis comes from multiple sources and most are well known to the maritime and security communities and well respected by them. For example, the ISPS Code, Octave and CRAMM form the basis for the maritime ICT security profile. This model uses a combination of the general ICT and social barriers drawn up from the findings of Chapters 1 and 2 and the 9 specific barriers from the data. The profile will be helpful in the real world in terms of informing attempts to counter actual and potential dangers.

7.3 Contribution to the literature

This research has considered secure ICT at sea with a particular focus on barriers. It has pointed to gaps in secure maritime ICT literature and to a scarcity of research into the potential impacts and consequences of incidents related to lack of ICT security that may occur at sea. In so doing, it has contributed to new knowledge in a number of important ways with the principal contribution being a model for a maritime ICT security profile. Protecting ICT assets is essential and this research has identified nine of the barriers to maritime ICT security, an understanding of which has been used in the maritime ICT security profile.

The findings of this research suggest that the maritime sector should acknowledge the existence of barriers to secure ICT to a much greater extent and adopt pro-active countermeasures that will help all mariners understand and deal with security issues. If security incidents are to be avoided, or at least contained, then adopting a profile approach will help security experts design and implement secure ICT more effectively. Additionally, the profile will help raise overall awareness across the maritime sector.

7.4 Intended audience and how others should use this work

The intended research audience includes those wishing to start their careers in the maritime sector or more experienced researchers reflecting on barriers and the nature of barriers. The audience for the practical results include all lawful mariners who wish to gain a better understanding of ICT security and how it might affect their organisation. Finally, for those working in the maritime sector where military and merchant co-operation required, this research will help situate their appreciation.

This work can be used in several ways by those working in the maritime sector and researchers working across domains. First, they could use the maritime profile to assess ICT assets and vulnerabilities within their own organisations and use the results to build an ICT security management plan. Second, the information gathered for ICT could be used to help with a ship's physical security plan. This could be part of a two way trade of information between ICT and physical security personnel to help reduce duplication of effort. Third, researchers could use the information contained in this thesis to reflect on barriers and perspectives on how barriers behave in different conditions and circumstances. Fourth, it can be used by those wishing to reflect on maritime ICT and maritime trade. Fifth, it can be used by those reflecting on practical ICT security in a land environment. Finally, there is sufficient information to generate maritime ICT security scenarios. Consider, for example, a situation where maritime ICT systems enact the priorities of float move fight. Routine operations can be broken down into distinct periods during which the location dependant aspects of barriers will come to the fore. Automated damage control terminals making pre-emptive reconfiguration of damage control equipment; machinery is running and selected in optimum states and conditions; intelligent work terminals storing and processing information; whilst communications nodes scan the electro-magnetic spectrum and select the most efficient channel to 'clear traffic'. The routine operations will also require integrated sensor data and information that can be generated in any part of the world. A list of the components of this situation is provided in Table 7.1 together with location dependant barriers.

Table 7.1: Components of a hypothetical return voyage. Secure ICT systems configured to meet prevailing conditions and circumstances.		
ICT systems that support the priorities of float move fight	Location	Barriers
Period 1	Alongside (Home) Mooring buoy At anchor	Barriers associated with connection to land lines. For example: 1. Threats from hackers and intruders 2. Threats from viruses, worms and Trojans 3. Absence of privacy of personal data 4. People who connect insecure machines to the Internet do not bear the full consequences of their actions 5. The ease with which computer users are deceived by fake websites 6. Many people say they value privacy yet act otherwise when online
Period 2	Exit (Day) Restricted in Ability to Manoeuvre Constrained by draft Passage Open waters, out of sight of land Sea areas of operations Coastal passage and 'choke points' Distress, urgency and safety	Transition from confidentiality integrity availability to secure ICT that supports float move fight: 1. Operational imperatives overriding security requirements 2. Tensions experienced between security experts and ICT users 3. Security limitations impeding business progress 4. Limited security training leading to repeated security incidents 5. Inadequate planning for recovery from disruption 6. Loss of ICT skills due to automation 7. Budget cuts lower moral and can reduce funding for security 8. Manpower cuts and information overload are cause problems of over work for little reward 9. Cancellation or delayed projects can require continued use of obsolete systems with inherent security shortfalls
Period 3	Alongside (Away)	Transition from secure ICT that supports float move fight to confidentiality integrity availability in an overseas environment 1. Unknown service providers 2. Crew behaviour
Period 4	Exit (Night)	Greater dependence on ICT for situational awareness 1. Jamming 2. Spoofing

7.5 Evaluation of the methodology and suggestions for further investigation

The research methodology was designed to allow an exploration of barriers in a maritime context with the aim of advancing understanding of security issues associated with the use of ICT systems in that context. The purpose of the methodology was to take the list of barriers identified from the literature as a starting point to develop an in depth view of 'real world' barriers to secure ICT in the maritime environment. To achieve this depth, one to one semi-structured interviews were conducted with Royal Navy and Merchant Navy personnel. The challenge of this approach was to find willing and able interviewees'. It had been planned to conduct certain interviews on-board ships. Although it would have helped to understand the

working environment, this did not happen because it was not possible to secure formal approval. The interview data was analysed using a grounded approach to allow characteristics to emerge from the data. A major output from this analysis was the realisation that the characteristics of barriers can very usefully be characterised as objective and subjective. For the Merchant Navy, a combination of observation of lectures and post lecture informal discussions were used. With hindsight, this component of the research would have benefited from a pre-course discussion with the course leader. Secondary data regarding Royal Navy and Merchant Navy security issues was also collected and data provided information that can be used for the generation of scenarios.

It is suggested that this research has raised two topics worthy of further investigation. First, a range of organisations from the maritime sector could be approached to take part in testing the utility of the security profile in the 'real world' and in so doing determine if the findings of this research are generalizable across military and commercial organisations. As part of this investigation, it is suggested that the subject population be extended to include people with limited maritime ICT security experience so that a broader picture can be established. (Those, for example, who use ICT but may not consider themselves to be subject experts.) Secondly, this research has described specific aspects of Royal Navy and Merchant Navy ICT security, and has revealed barriers, their characteristics and their attributes. However, these descriptions do not explain why a barrier is what it is; why does a barrier behave the way it does in certain circumstances but not others? This type of investigation would require a revised methodology and a new data collection effort.

The aim of the investigation would be to develop a theory of barriers to ICT security in the maritime sector.

References

ABC News (1991). Cruise Ship Sinks; Greek cruise ship Oceanos sinks off the coast of South Africa. *In:* DONALDSON, S. (ed.). New York: ABC News.

Abell, W. & Lim, L. (1996). *Business use of the Internet in New Zealand: an exploratory study* [Online]. Canterbury: Lincoln University. Available: http://ausweb.scu.edu.au/aw96/business/abell/paper.htm [Accessed 1 June 2009].

Alberts, C. & Dorofee, A. (2003). *Managing Information Security Risks,* Boston, Pearson Education.

Allen, J. (2005). Governing for enterprise security: networked systems survivability program. Pittsburgh: Carnegie Mellon University.

Amalberti, R. & Auroy, Y. (2005). Five system barriers to achieving ultrasafe health care. *Annals of Internal Medicine,* 142, 756-764.

Anderson, R. & Moore, T. (2009). Information security: where computer science, economics and psychology meet. *Philosophical Transactions of the Royal Society,* Mathematical, physical and engineering sciences, 2717-2727.

Anjum, Z. (2008). Singapore port becomes wireless-wise. Network World.

Baert B (1998). The use of IT in shipping: a company view improving shipping company performance through information technology. *Seminar proceedings.* London: The Nautical Institute.

Baily, C. (2011). Mumbai High North Platform Fire, India.

Ball, K. (2010). Data protection in the outsourced call centre: an exploratory case study. *Human Resource Management Journal,* 20, 294-310.

Baltic Exchange. (2011). *A history of the Baltic Exchange* [Online]. London. Available: http://www.balticexchange.com/ [Accessed 15 Jan 2011].

Banlaoi, R. (2005). Maritime terrorism in southeast Asia: The Abu Sayyaf Threat. *Naval War College Review,* 58, 63-80.

Bateman, T. (2013). *Police warning after drug traffickers' cyber-attack* [Online]. London: BBC. [Accessed 21 October 2013].

Berghel, H. (2008). Faith-Based Security. *Communications of the ACM,* 51, 13-17.

Bignell, V. & Fortune, J. (1984). *Understanding Systems Failures,* Manchester, Manchester University Press.

Black, J. & Ulrich, D. (1999). The new frontier of global HR. *In:* P, J. & R, M. (eds.) *The global HR manager: creating the seamless organisation.* London: Chartered Institute of Personnel and Development.

Blumer, H. (1969). *Symbolic interactionism,* Englewood Cliffs, Prentice Hall.

Bradbury, D. (2013). New wave of technology. *E&T Engineering and Technology.* Stevenage: IET Services Limited.

Burton, E. (2008). Report into the loss of MOD personal data. *In:* MINISTRY OF DEFENCE UK (ed.). London: HMSO.

Cabinet Office. (2005). *The Infosec competencies 2005* [Online]. London: Central Sponsor for Information Assurance. Available: http://www.cabinetoffice.gov.uk [Accessed 28 June 2007].

Cahill, R. (2002). *Strandings and their causes,* London, The Nautical Institute.

Caralli, R. (2004). Managing for Enterprise Security. *In:* DEFENSE (ed.) *Networked Systems Survivability Program.* Pittsburgh: Carnegie Mellon University.

Caralli, R. & Young, L. (2008). Expanding the OCTAVE Method to Perform Continuous Risk Management of Information and Operational Security *In:* LINGER, R. (ed.). Pittsburgh: Software Engineering Institute.

Carnegie Melon Institute. (2007). *CERT CC Software Engineering Institute web site* [Online]. CERT CC. Available: http://www.cert.org [Accessed 12 Jul 2007].

Carnegie Melon Institute. (2013). *20 security controls version 4.0* [Online]. Pittsburgh: Carnegie Mellon University. Available: www.cert.org/mswa/download/SwA-Course/SwA%20Execs%20Basic%20Concepts%20of%20Security.pdf [Accessed 20 September 2013].

Casey, E. (2000). *Digital Evidence and Computer Crime,* London, Cambridge University Press.

CESG. (2008a). *National Technical Authority for Information Assurance* [Online]. Cheltenham: CESG. Available: http://www.cesg.gov.uk/index.shtml [Accessed 11 May 2008].

CESG (2008b). *HMG Information Assurance Maturity Model,* Cheltenham, CESG.

CESG (2009). HMG Information Assurance Standard No. 1. Technical Risk Assessment. Cheltenham: CESG.

Chaturvedi, A. (2010). Maritime piracy and maritime terrorism must be tackled with a unified effort. *U.S. Naval Institute Proceedings,* 136, 24-28.

Chitura, T., Mupemhi, S., Dube, T. & Bolongkikit, J. (2008). Barriers to electronic commerce adoption in small and medium enterprises. A critical literature review. *Journal of Internet Banking and Commerce,* 13.

Clark, M. (1997). *Networks and Telecommunications, Design and Operations,* Chichester, John Wiley & Sons.

Clarke, R. & Knake, R. (2010). *Cyber War.The Next Threat to National Security and What to Do About It,* New York, Harper Collins.

Close, J. (2013). *Astrium's secure milsatcoms now cover the world* [Online]. London. Available: http://www.eads.com/eads/int/en/news/press.20130416_astrium_milsatcom.html [Accessed 1 May 2013].

Collins, P. (2002). *Virtual and networked organisations,* Tulsa, Capstone.

Collins, P. & Hogg, J. (2003). The ultimate distributed workforce: the use of ICT for seafarers. *AI & Soc,* 18.

Collins, R. & Hassan, D. (2009). Applications and Shortcomings of the Law of the Sea in Combating Piracy: A South East Asian Perspective *Journal of Maritime Law & Commerce,* 40, 89-113.

Corbin, J. & Strauss, A. (2008). Basics of qualitive research: techniques and procedures for developing grounded theory. 3 ed. Thousand Oaks: Sage Publications Inc.

Davies, A. & Parfett, M. (2000). *Seafarers and the Internet: e-mail and seafarers' welfare* [Online]. Cardiff. Available: http://www.sirc.cf.ac.uk/ [Accessed 1 December 2012].

Davis, Z. (2010). Weaving a Web 2.0 security strategy. *Baseline Magazine* [Online]. Available: http://www.baselinemag.com [Accessed 12 Deceber 2012].

Demiray, U. & Sharma, R. C. (2009). Ethical practices and implications in distance education: an introduction. *In:* DEMIRAY, U. & SHARMA, R. C. (eds.) *Ethical Practices and Implications in Distance Learning.* Hershey: Information Science Reference.

Dunlop, J. & Smith, D. (1994). *Telecommunications engineering,* London, Chapman & Hall.

Dunston, G. (2010). *Shortfalls of GMDSS* [Online]. Available: http://www.gmdss.com.au [Accessed 10 December 2010].

Dutta, A. & McCrohan, K. (2002). Management's Role in Information Security in a Cyber Economy. *California Management Review,* 45, 67-87.

Ebrahim, Z. & Irani, Z. (2005). E-government adoption:architecture and barriers. *Business Process Management Journal,* II, 589-611.

Economist (1999). Dead men tell no tales: South Sea Piracy *Economist.* London: Economist.

ENISA (2011). Analysis of cyber security aspects in the maritime sector. Heraklion: European Network and Information Security Agency.

Fleisch, E., Senger, E. & Thiesse, F. (2005). Ubiquitous network societies: Thier impact on the telecommunications industry. Zurich: International Telecommunications Union.

Foddy, W. H. (1995). *Constructing questions for interviews and questionnaires: theory and practice in social research,* Cambridge, Cambridge University Press.

France, L. & Beaty, L. (1998). Layers of motivation: individual orientations and contextual influences. *In:* BROWN, S., ARMSTRONG, S. & THOMPSON, G. (eds.) *Motivating Students.* Birmingham: Kogan Page.

Gaitskell, R. (1998). The sheriff of cyberspace: law and the Internet. *IEE Engineering Management Journal,* 8, 261-269.

Geertz, C. (1973). *The Interpretation of Cultures,* New York, Basic Books.

Gefen, D. & Pavlou, P. (2002). Egovernment adoption. *Americas Conference on Information Systems.* Tampa.

Gill, M. (1995). Issues in Maritime Crime: Mayhem at Sea. Leicester: National Criminal Justice Reference Service.

Glavovic, B. & Boonzaier, S. (2007). Confronting coastal poverty: Building sustainable coastal livelihoods in South Africa. *Ocean & Coastal Management,* 50, 1-23.

Golden-Biddle, K. & Locke, K. (1993). Appealing work: an investigation of how ethnographic texts convince. *Organisational Science,* 4, 595-616.

Golding, P. (2008). *Next generation wireless applications,* Chichester, Wiley.

Goldsmith, A. (2005). *Wireless communications,* Cambridge, Cambridge University Press.

Gratton, D. A. (2007). *Developing practical wireless applications,* Oxford, Elsevier.

Guardian. (2011). Legacy of the Torrey Canyon, 18 March 1967. *The Guardian.*

Hannigan, R. (2008). Data Handling Procedures in Government: Final Report. *In:* CABINET OFFICE (ed.). London: HMSO.

Harris, B. & Hunt, R. (1999). TCP/IP security threats and attack methods. *Computer Communications,* 22, 885-897.

Hastings, J. (2009). Geographies of state failure and sophistication in maritime piracy hijackings. *Political Geography;,* 28, 213-223.

Herath, H. S. B. & Herath, T. C. (2008). Investments in Information Security: A Real Options Perspective with Bayesian Postaudit. *Journal of Management Information Systems,* 25, 337-375.

Hesse, H. & Charalambous, N. (2004). New Security Measures for the International Shipping Community. *WMU Journal of Maritime Affairs,* 3, 123-138.

Hill, J. (2000). Bypassing Firewalls: Tools and Techniques. *12th Annual FIRST conference.* Chicago: FIRST.

HMG. (2007). *CRAMM web site* [Online]. London: HMG. Available: http://www.cramm.com [Accessed 16 Mar 2007].

Horizon Scanning Centre. (2013). *Foresight, Government Office for Science* [Online]. London: Government Office for Science. Available: http://www.bis.gov.uk/assets/foresight/docs/horizon-scanning-centre/futuresinpolicyguidance.pdf [Accessed 10 July 2013].

Hurlburt, K. (2011). The Human Cost of Somali Piracy. Colorado.

International Maritime Organisation (2003). *ISPS Code: International Ship & Port Security Code and SOLAS Amendements 2002,* London, International Maritime Organisation.

International Maritime Organisation. (2004). *The International Ship and Port Facility Security (ISPS) code* [Online]. IMO. Available: http://www.imo.org [Accessed 2 January 2008].

International Maritime Organisation. (2009). *IMO team site* [Online]. IMO. Available: http://www.imo.org [Accessed 14 September 2009].

International Naval Safety Association. (2011). *Web site for the International Naval Safety Association* [Online]. London: Lloyd's Register. Available: http://navalshipcode.org/ [Accessed 13 October 2011].

International Organization for Standardisation. (2008). *ISO 27000 series* [Online]. Geneva: ISO. Available: http://www.iso.org [Accessed 2 November 2008].

International Telecommunications Union. (2011). *Cyber security, ITU-T Recommendation X.1205* [Online]. Available: http://www.itu.org [Accessed 16 December 2012].

Internet Engineering Task Force. (2007). *Internet Engineering Task Force web site* [Online]. IETF. Available: http://www.ietf.org [Accessed 11 May 2007].

Jeory, T. & Glannangell, M. (2011). Pirates outwit us, says Royal Marine. *Sunday Express.*

Kalsson, J. (2011). Detection and Prevention of Wormhole Attacks in Mobile Ad hoc Networks (MANET). *Research Student Event, The Open University.* Milton Keynes.

Khalil, R., Zaki, F., Ashour, M. & Mohamed, M. (2010). A Study of Network Security Systems. *International Journal of Computer Science and Network Security,* 10 204-212.

Kim, D., Jung, Y. & Chung, T. (2005). PRISM: A Preventive and Risk-Reducing Integrated Security Management Model Using Security Label. *Journal of Supercomputing.*

Kropp, T. (2006). System threats and vulnerabilities [power system protection]. *Power and Energy Magazine,* 4, 46-50.

Krutz, R. I. & Vines, R. D. (2003a). *Advanced CISSP Prep Guide Exam Q&A,* London, Wiley.

Krutz, R. L. & Vines, R. D. (2003b). *The CISSP Prep Guide,* London, Wiley.

Krutz, R. L. & Vines, R. D. (2010). *Cloud Security: A Comprehensive Guide to Secure Cloud Computing,* Indianapolis, Wiley Publishing.

Kshetri, N. (2006). The simple economics of cybercrimes. *Security & Privacy, IEEE* 4, 33-39.

Kvale, S. (1996). *Interviews: An Introduction to Qualitative Research Interviews,* Thousand Oaks, Sage Publications.

Lawson, R., Alcock, C., Cooper, J. & Burges, L. (2003). Factors affecting adoption of electronic technologies by SMEs: an Australian study. *Journal of small business and enterprise development,* 10, 265-276.

Lees, G. D. & Williamson, W. G. (2009). *Handbook for Marine Radio Communication,* London, Informa Law.

Leon, O., Hernandez, J. & Soriano, M. (2010). Securing cognitive radio networks. *International Journal of Communication Systems,* 23.

Lloyd's List. (2011). *Maritime & Transport News Portal* [Online]. Available: http://www.lloydslist.com [Accessed 30 January 2011].

Lloyd's Register. (2013). *Lloyd's Register web page* [Online]. London: Lloyd's Register Group Services Limited. Available: http://www.lr.org/default.aspx [Accessed 21 October 2013].

Luo, J., Joshi, D., Yu, J. & Gallagher, A. (2011). Geotagging in multimedia and computer vision-a survey. *Multimedia Tools & Applications,* 187-211.

MacGregor, R. C. & Vrazalic, L. (2004). Electronic commerce adoption in small to medium enterprises (SMEs): a comparative study of SMEs in Wollongong (Australia) and Karlstad (Sweden).

Mann, I. (2008). Hacking the human. *IET Engineering and Technology,* 3.

McAfee. (2011). *McAfee web site* [Online]. London: McAfee. Available: http://www.mcafeeprotection.com/UK/index.asp [Accessed 21 April 2011].

McGee, A. R., Bastry, F. A., Chandrashekhar, U., Vasireddy, S. R. & Flynn, L. A. (2007). Using the Bell Labs security framework to enhance the ISO 17799/27001 information security management system. *Bell Labs Technical Journal,* 12, 39-54.

Medjahed, B., Rezgui, A., Bouguettaya, A. & Ouzzani, M. (2003). Infrastructure for e-government web services. *IEEE Internet Computing,* 7, 58 -65.

Mersey (1912). British Wreck Commissioner's Inquiry: Report on the Loss of the "Titanic.". *In:* BRITISH WRECK COMMISSIONER (ed.). London: HMSO.

Miles, M. B. & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook,* Thousand Oaks, Sage.

Ministry of Defence UK (2004). *British Maritime Doctrine,* London, HMSO.

Ministry of Defence UK (2009). *Defence manual of CIS security,* London, HMSO.

Ministry of Defence UK. (2010a). *Conditions for Full Time Reserve Service (FTRS)* [Online]. London. Available: http://www.mod.uk [Accessed 4 July 2010].

Nanda, V. (1967). Torrey Canyon disaster: Some legal aspects. *Denver Law Journal.* Denver.

NATO. (2010). *An Introduction to Allied Communications* [Online]. Washington DC: Combined Communications and Electronics Board. Available: http://jcs.dtic.mil [Accessed 6 January 2010].

NATO (2011). *ANEP77 Naval Ship Code,* Bristol, NATO.

NECCC (2000). E-Government Strategic Planning. Las Vegas: National Electronic Commerce Coordinating Council.

New Zealand Government. (1999). *Y2K - fundamental design flaw?* [Online]. NZ Government. Available: http://www.maritimenz.govt.nz/publications/miscnotices [Accessed 11 May 2006].

Nissan (2012). Company profile. Yokohama: Nissan Motor Co., Ltd.

Noe, T. H., Rebello, M. J. & Wang, J. U. N. (2006). The Evolution of Security Designs. *Journal of Finance,* 61, 2103-2135.

OFCOM. (2007). *Electro-magnetic spectrum management* [Online]. London: OFCOM. Available: http://www.ofcom.org.uk [Accessed 11 May 2007].

Oxford English (1996). Oxford Reference English. *In:* PEARSALL, J. & TRUBLE, B. (eds.) *The Oxford English Reference Dictionary.* Second ed. Oxford: Oxford University Press.

Patel, S., Bhatt, G. & Graham, J. (2009). Improving the cyber security of scada communication networks. *Communications of the ACM,* 7, 139-142.

Pfleeger, C. P. (1997). *Security in Computing,* New Jersey, Prentice Hall.

Pham, P. (2010). Putting Somali piracy in context. *Journal of Contemporary African Studies,* 28, 325-341.

Megastructures - Singapore, the world's busiest port, 2008. Television. Directed by Phang, E.: National Geographic.

Pidgeon, N. (2010). Systems thinking, culture of reliability and safety. *Civil Engineering and Environmental Systems,* 27, 211-217.

Piggin, R. (2010). The reality of cyber terrorism. *E&T Engineering & Technology.* Stevenage: IET.

Pillai, D. & Andley, P. (2010). Information security threats. *Disaster management and security.*

Plaga, R. (2009). Biometric keys: suitable use cases and achievable information content. *International Journal of Information Security,* 447-454.

Post Office (1975). Handbook for Radio Operators Working Installations Licensed by The Home Office. London: Her Majesty's Stationary Office,.

Potter, S. (2006). *Doing postgraduate research,* London, Sage.

Preece, R. (1994). *Starting research: An introduction to academic research and dissertation writing,* London, Pinter Publishers.

Price, J. (1969). *A tribute to fifty years' work for seafarers: the International Labour Organisation Seafarers' Code,* London, Co-operative Printing Society Ltd.

Price, J. (1972). *An abuse that must be ended,* Manchester, Trafford Press Ltd.

Public Accounts Committee (2008). Defence Information Infrastructure: First Report of Session 2008–09. *In:* DEFENCE COMMITTEE (ed.). London: The Stationery Office Limited.

Public Accounts Committee (2013). Defence and Cyber–Security: Government Response to the Committee's Sixth Report of Session 2012–13. *In:* DEFENCE COMMITTEE (ed.). London: The Stationery Office Limited.

QinetiQ Ltd. (2006). *QinetiQ takes NEC capability to sea* [Online]. QinetiQ. Available: http://www.qinetiq.com [Accessed 12 May 2006].

Qingxiong, M. & Pearson, J. M. (2005). ISO 17799: "BEST PRACTICES" IN INFORMATION SECURITY MANAGEMENT? *Communications of AIS,* 2005, 577-591.

Rackley, S. (2007). *Wireless networking technology,* Oxford, Elsevier.

Records from BBC News Archive (1967). Torrey Canyon, largest vessel ever to be wrecked. London.

Records from BBC News Archive (1982). Argentines destroy HMS Sheffield, 4 May 1982. London.

Records from BBC News Archive (1987). Herald of Free Enterprise was no accident. London.

Records from BBC News Archive. (2012). *The Olympic fear factor behind securing the Games* [Online]. London. Available: http://www.bbc.co.uk/news/magazine-18923741 [Accessed 1 May 2013].

Rees, J. & Allen, J. (2008). The State of Risk Assessment Practices in Information Security: An Exploratory Investigation. *Journal of Organizational Computing & Electronic Commerce,* 18, 255-277.

Reynolds, G. (2003). *Ethics in Information Technology,* Boston, Thomson.

Richards, S. (2013). Electronics, Navigational Aids and Radio Theory for Electrotechnical Officers. 1st ed. London: Blomsbury.

Rishi, L. (2005). Presence and its effect on network *IEEE International Conference on Personal Wireless Communications*, 368 -372

Robins, G. (2001). E-government, information warfare and risk management: an Australian case study. *2nd Australian Information Warfare Security Conference.* Perth.

Rothe, D. & Collins, V. (2011). Somalia piracy. *Contemporary Justice Review,* 14, 329-343.

Roumboutsos, A., Nikitakos, N. & Gritzalis, S. (2005). Information technology network security risk assessment and management framework for shipping companies. *Maritime Policy & Management: The flagship journal of international shipping and port research,* 32, 421-432.

Royal Navy (1982). The loss of HMS Sheffield. Board of Enquiry.

Royal Navy (1988). Collision between HMS Southampton and MV Torbay 3 Sept 1988 - Board of Inquiry report. Northwood: Royal Navy.

Royal Navy (2002). Report into the grounding of HMS Nottingham on 7 July 2002. *In:* PORTSMOUTH, C. (ed.). Portsmouth: Royal Navy.

Royal Navy. (2009). *Second Sea Lord's Personnel Standards of Conduct and Behavior* [Online]. Portsmouth: Royal Navy. Available: http://www.royalnavy.mod.uk [Accessed 1 May 2009].

Royal Navy. (2013). *UKMTO contact details* [Online]. London: MODUK. Available: http://www.royalnavy.mod.uk/Operations/Maritime-Security/Keeping-the-Sea-Lanes-Open/UK-Maritime-Trade-Operation [Accessed 1 February 2013].

Saunders, M., Lewis, P. & Thornhill, A. (1997). *Research methods for business students,* London, Pitman Publishing.

Savory, C. & Fortune, J. (2013). NHS Adoption of NHS-developed Technologies. Final report. NIHR Service Delivery and Organisation programme; 2013. Southampton: National Institute for Health Research.

Schiller, J. H. (2003). *Mobile communications,* London, Addison Wesley.

Schneier, B. (1996). *Applied Cryptography,* New York, John Wiley & Sons.

Schneier, B. (2000). *Secrets and lies digital security in a networked world,* New York, John Wiley & Sons.

Schultz, E. E. & Shumway, R. (2002). *Incident Response,* Indianapolis, New Riders.

Sheen (1987). MV Herald of Free Enterprise: Report of Court No. 8074, Formal Investigation. London: Department of Transport.

Siemans. (2007). *How CRAMM works* [Online]. London: Siemens Enterprise Communications Limited Available: http://www.siemens.com/ [Accessed 16 March 2007].

Silverman, D. (2000). *Doing qualitative research,* London, Sage.

Simpson, O. (2009). Open to people, open with people: ethical issues in open learning. *In:* DEMIRAY, U. & SHARMA, R. (eds.) *Ethical Practices and Implications in Distance Learning.* Hershey: Information Science Reference.

Sluiman, F. J. (2010). Encrypt Naval Communications with Merchant Ships. *U.S. Naval Institute Proceedings.* Annapolis: U.S. Naval Institute.

Smith, M. (1998). *Station X,* London, McMillan.

Smith, W., Borrell, J. & Fischer, D. (1985). The voyage of the Achille Lauro A Mediterranean pleasure cruise turns into a 52-hour nightmare at sea. *Time.*

Stallings, W. (2007). *Data and Computer Communications,* New Jersey, Pearson Education.

Stanfield, M. & Grant, K. (2003). An investigation into issues influencing the use of the Internet and electronic commerce among small-medium sized enterprises. *Journal of electronic commerce research,* 4, pp: 15-33.

Stavanger Museum (2005). A history of the production platform Alexander L. Kielland. Stavanger.

Stopford, M. (2009). *Maritime Economics,* Oxon, Routledge.

Storey, J. & Buchanan, D. (2007). Patient safety and clinical governance. Milton Keynes: The Open University and Cranfield School of Management.

The Law Society. (2006). *Society welcomes clarification of law over corporate manslaughter Legislation creating a new criminal offence of corporate manslaughter* [Online]. London: The Law Society. Available: http://www.lawsociety.org.uk [Accessed 1 February 2009].

The National Business Review. (2009). *French Navy surrenders to Conficker, 12 Feb 2009* [Online]. Available: http://www.nbr.co.nz/ [Accessed 27 October 2009].

The Open University (2008a). M886 Unit 1 Postgraduate ICT and Computing: Information security management. 2nd ed. Milton Keynes: The Open University.

The Open University (2008b). M886 Technical Appendix. Milton Keynes: The Open University.

The Open University (2008c). M886 Unit 2 Postgraduate ICT and computing: Information security management. 2nd ed. Milton Keynes: The Open University.

Tulloch, J. & Lupton, D. (2003). *Risk and everyday life,* Gateshead, Sage Publications.

Turner, B. A. (1983). The use of grounded theory for the qualitative analysis of organisational behaviour. *Journal of Management Studies,* 20, 333-348.

van der Lubbe, J. (1998). *Basic Methods of Cryptography,* Cambridge, Cambridge University Press.

Wall, D. S. (2007). *Cybercrime,* Cambridge, Polity Press.

Walsham, G. (2006). Doing interpretive research. *European Journal of Information Systems,* 15, 320-330.

Watson, M. H. (1995). *Disasters at sea,* Sparkford, Haynes Publishing.

Watts, J. (2010). Teaching a distance higher education curriculum behind bars: challenges and opportunities. *The Journal of Open and Distance Learning,* 25(1), 57-64.

Whitman, M. E. & Mattord, H. J. (2007). *Principles of Incident Response and Disaster Recovery,* Boston, Thomson.

Witten, I. & Frank, E. (2005). *Data mining, practical machine learning tools and techniques,* San Francisco, Morgan Kaufmann.

Yin, R. (2003). *Case study research design and methods,* Thousand Oaks, Sage Publications.

Zeadally, S., Sklavos, N., Rathakrishnan, M. & Fowler, S. (2007). End-to-End Security Across Wired-Wireless Networks for Mobile Users. *Information Systems Security,* 16, 264-277.

Zeichner, L. M. (2001). Developing an overarching legal framework for critical service delivery in America's cities: three recommendations for enhancing security and reliability. *Government Information Quarterly,* 18, 279-291.

Zwicky, E. D., Cooper, S. & Chapman, B. (2000). *Building Internet Firewalls,* Sebastopol, O Reilly.

Appendix A

Guidelines used in this research

Research question: **What are the barriers to achieving information and technology security in a maritime environment?**
Interview topics: **Information Assurance, people and technology.**
The purpose of the research and anticipated audiences: **To advance the understanding of information and technology security at sea. This work will include physical security aspects and is being conducted for the benefit of all lawful mariners.**
Informed permission will be sought for each person interviewed or observed. All participants will be briefed separately prior to the commencement of any formal or informal interview or observation.
Interviews will be conducted on the principle of confidentiality. Permission will be sought to take notes and make audio recordings of each interview. The notes will be summarised in a database for use as agreed below.
Use of the data will be negotiated with participants on specific criteria and within specific timelines. The data will be used for statistical purposes and will contribute to more detailed analysis such as Cognitive Mapping or Grounded Theory. Your data may be used in papers and journal articles. The thesis itself is due for completion in September 2011.
No data will be used that a participant asks to be kept in confidence.
Participants will be asked at the end of the interview for permission to use their data and if anything needs to be excluded.
Participants will have an opportunity to see their data and how comments and observations about them are reported in the context of the case study. Participants may edit and add in, if necessary, criteria for accuracy, relevance and fairness (The appropriate section of the database will be forwarded for consideration and approval).
Direct quotation and attributed judgements in articles, journals and reports require the explicit permission of the participant.
Permission will be sought for access to documents, files and correspondence. These items will not be copied without explicit permission.
Non-attributable data and information used in summarising findings across projects or in raising general issues about the findings does not require specific clearance.

Appendix B

Royal Navy data and mapping

SY1 27th Feb 2009

Author's note: This interview was conducted as part of the scoping exercise described in Chapter 3. As such, the question numbering used here correspond to the numbering used for the main interviews and not the numbering used during this pilot interview.

Data block and question	Interviewee's opinions of maritime environment and ICT security	Researcher's interpretation of interviewee's opinions	Research code
A Q1	The new technology will support not only the critical safety at sea, but will support the business drivers, certainly in the Merchant Service, which will be reducing operating costs whilst maximising profit. In a military context greater faith in the ships fighting capability will be preserved. Modern technology is considerably more reliable and easier to maintain because it is a swop out swop in.	1. Network and information security is a challenge. 2. ICT has critical role to play. 3. Reducing operating costs can lead to reduction in money spent on ICT security. 4. Role of ICT continues to develop. 5. Reliability of ICT may point to other problems with security.	1. Network 2. Identify critical systems 3. Operating costs 4. Changing roles of IT 5. Reliability
B Q1	Communications technology has allowed a greater coming together of disparate systems used to maintain the vessel, its propulsion systems, its navigation systems and greater information sharing between organisations.	1. Integration of on-board control systems. 2. Enables organisations to share information if they want to.	6. Network 7. Control systems 8. Information sharing
C Q3	We have moved on quite considerably from the days of the Titanic disaster where it was very basic wireless technology and line of sight communications to being able to have world-wide communications real-time and instantaneous. So overall the new technology is supporting the business in all aspects.	1. Communications enable world-wide operations. 2. Able to communicate anytime, anywhere. 3. Supports all aspects of business.	9. World-wide 10. Mobile 11. Communications 12. Real time 13. Instantaneous 14. Support to operations
D Q7	Being a cynic? Where we have grown up over the last twenty years with technological solutions we haven't necessarily thought enough about the impact if that solution was not there.	1. Greater dependence on technical solutions. 2. Lack of fall-back options.	15. Support to operations 16. Dependence on technology 17. Systems failure 18. Impact
E Q7	Navigation skills are not necessarily taught any longer and there is the reliance on GPS satellite technologies which because they are nothing more than a computer could be attacked and taken out of service in which case we could finish up with a lot of ships scattered throughout the world and nobody knows how to get them home again.	1. Situational awareness depends on technical solutions. 2. Lack of fall-back options. 3. Loss of command and control	19. Situational awareness 20. Dependence on technology 21. Failure 22. Impact 23. Command and control
F Q7	Even within an engineering context engineers have been brought up to rely on IT to diagnose problems and indeed to rectify problems. Without that IT a lot of engineering solutions will not be apparent.	1. Technology used for mechanical and electrical fault diagnosis. 2. Loss of engineering skills.	24. Engineering needs IT 25. Dependence on technology 26. Loss of engineering skills 27. Systems failure 28. Impact
G Q7	Communications, lose the IT that provides the internet type communications do we still retain the skills for radio frequency communications or line of sight communications? The loss of traditional communications skills as a result of technology is a potential business disabler.	1. In the event of a systems failure, the lack of fall-back because of the loss of traditional radio communication skills will present problems.	29. Systems failure 30. Impact

Continued ....

SY1

Data block and question	Interviewee's opinions of maritime environment and ICT security	Researcher's interpretation of interviewee's opinions	Research code
H Q7	Whilst I appreciate the reason for the reduction of training within the traditional skills because they were manpower intensive which IT tends to be; the opposite for business continuity we still need to retain those skills	1. Need to reduce personnel costs. 2. Loss of traditional skills 3. Need to retain skills as fall-back	31. Operating costs 32. Loss of skills 33. Skills for contingency
I Q7	It has been said that children leaving school will have lost the ability to write, certainly lost the ability to use pens and paper because of their reliance on IT.	1. Loss of traditional skills	34. Loss of skills 35. Skills for contingency
J Q7	Impact could be catastrophic to the business which in a military context could lead to a loss of life in a business context could result in a company having to file for bankruptcy.	1. Loss of IT could be catastrophic in military and commercial context.	36. Catastrophic
K Q8	Broadly speaking our maritime cousins face exactly the same problems as a terrestrial based system	1. Afloat and ashore face similar problems	37. Context based
L Q8	For example, if there were a malicious software attack that originated in the Far East, then a UK based fixed system would be attacked possibly 3 or 4 hours after a fixed place in the Far East. However, a UK ship in the Far East will be attacked at that time. They face the same threats and vulnerabilities and therefore the risk is the same perhaps just in different time scales.	1. Threat from malicious software similar but time scales may differ	38. Threat time scale
M Q8	The concept of the platform being in a salt water environment; electricity and water do not mix very well. The corrosive effect of salt water and the atmosphere on metallic objects is far greater and corrosion on a key component on an IT system will be more catastrophic. Special consideration has to be made for the corrosive effect of salt water.	1. Salt water corrosion 2. Electrical equipment surrounded by water	39. Corrosion 40. Physical protection 41. Electrical protection
N Q8	Working conditions were there isn't as much free space around the equipment down to and including a key board is an issue.	1. Working environment not ideal 2. Limited IT available	42. People's working conditions 43. Limited IT assets
O Q8	The availability and compatibility of spares is an issue.	1. Are the correct spares available?	44. Maintenance
P Q8	Satellites issues associated with atmospherics and change of position.	1. Electro-magnetic environment 2. Satellite tracking	45. Interference
Q Q8	There isn't much time to get software patches which may or may not be critical. How do you get soft patches if you are at sea and have been attacked by a virus and are on a distributed network and as part of the network defence you have been disconnected from the network?	1. Zero day attack 2. How to get software fix if network not available	46. Speed of attack 47. Software patches
R Q8	The way you would get the fix is as an e-mail attachment: that could have interesting outcomes.	1. Lack of fall-back	48. Contingency
S Q8	Network Enable Capability has the potential to put an additional burden on staff because the electronic environment in which we and others are working is greater and the adversary will be able to hide where he is coming from and as everything joins together for information sharing the impact on the business from a loss of that capability could be greater.	1. Work load increasing due to the actions of the ill-disposed. 2. Increasing capability of the ill-disposed. 3. If business carried out in a networked and information sharing environment then loss of capability at sea could have a greater impact than similar occurrence on land.	49. People's working conditions 50. Cyber warfare 51. Impact

Continued ....

SY1

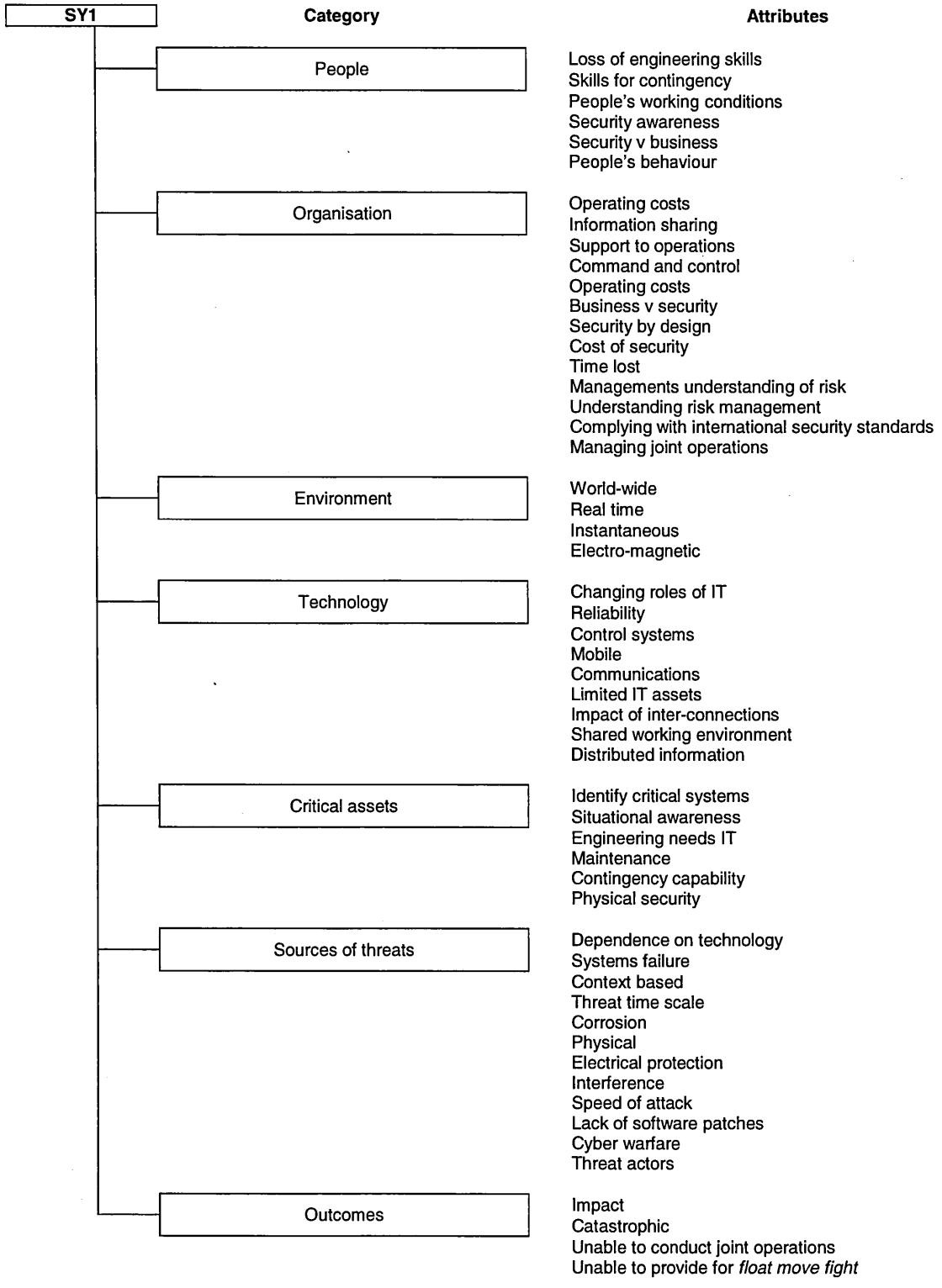
Data block and question	Interviewee's opinions of maritime environment and ICT security	Researcher's interpretation of interviewee's opinions	Research code
T Q8	The threats will be the same: there are only about a dozen basic types of malicious software however there are several thousand variations on a theme. As we join together perhaps we need to take stock of who the threat actor is: keep your enemies close but keep your friends closer'.	1. Threats are the same in all environments. 2. Must understand who or what poses the threats and then understand how those threats may be carried out.	52. Threat assessment 53. Threat actors 54. Vulnerability assessment
U Q8	Yesterday's terrorist is today's freedom fighter and tomorrow's politician. Know your enemy. The threat will be the same it may have a different complexion.	1. Keep up to date with current threat actors. 2. Monitor how threats change and evolve	55. Threat actors
V Q11	I see a greater need for security risk management. We security professionals could adopt the head in the sand approach 'The answers no, now what is the question?' The effect that has on business is potentially catastrophic. We need to be firmly embedded in business; we need to have a good understanding of business and the business needs to understand where we are coming from.	1. Security must keep pace with the operational requirements of the business. 2. Business must keep pace with current security requirements.	56. Security v business 57. Business v security
W Q11	It is business information that needs protecting. Information is the most valuable to the organisation after its work force and the business needs to understand that and from the outset of any programme work with the security professional rather than allowing security to be bolted on at the end when it becomes costly and those costs may well be disproportionate.	1. Information should be regarded as an important asset and protected as such. 2. Security should be built in, not added as an expensive after thought.	58. Awareness 59. Security by design 60. Cost of security 61. Time lost
X Q12	I have no direct experience of it. What I do have experience of is where systems are coming together what is to one system is a small risk and will be accepted in that business area having a major impact on another and therefore presents a greater risk to other business areas. If those areas are within an entire single organisation, I accept that the cumulative effect could be catastrophic.	1. When systems exchange information in situations in which they were not designed to do so, then the risk of unforeseen consequences can be catastrophic.	62. Security by design 63. Impact of inter-connections
Y Q12	I am not sure whether businesses fully understand the individual risks they are carrying may have an impact on somebody else. At senior level, I am not sure they understand the cumulative effect. You only need to look at recent events in the financial world to show exactly what I mean by that. That I think is an awareness issue and the cultural issue: we have never had a problem so why should I worry about it now and why should I worry about what I am doing in terms of somebody else's business. So it's the parochial nature of business units.	1. Senior management not fully aware of the cumulative effect of risk. 2. Awareness and cultural issues of shared working environment.	64. Managements understanding of risk 65. People's behaviour 66. Shared working environment

Continued ....

SY1

Data block and question	Interviewee's opinions of maritime environment and ICT security	Researcher's interpretation of interviewee's opinions	Research code
Z Q12	These views have been much the same since I got into this business. Although 20 years ago information held on the PC ITSy then was lock away the hard disc. Now with systems storing information in data warehouses local servers or whatever, we have seen a slight shift. People are less reluctant to store things locally then they were although when it was locked away with disc they were more likely to lock the key board. Now they will get up and walk away because the system will do it after 30 minutes and there is no information there it is all on the server it does not matter the machine is still accessible. There are some positives and some negatives. We are getting there slowly towards the stage where people are realising that we all have a part to play in security and protecting information. But we need to wait another half a generation before it becomes effective so the 'Facebook' generation of IT literate juniors take up the senior management positions.	1. When systems where standalone and not mobile in the way they are today, then it was possible to lock away a PC or even remove a hard drive and store it in a safe. 2. Now, servers can be off-site, devices are mobile and have wireless connectivity which changes the nature of IT security. 3. Awareness of this change is slow to take hold. 4. Even when awareness in place, people's behaviour still tends towards the 'take the easy way' approach. 5. Understanding will come, but is some years off.	67. Physical security 68. Distributed information 69. Security awareness 70. People's security behaviour
AA Q13	It has been suggested that perhaps we do that [use non MODUK methodologies] and there was a suggestion within government that the financial world understands risk management quite well and we should perhaps be learning from them: I need say no more.	1. Although risk management is said to be well understood, this is not always the case.	71. Understanding risk management
BB Q13	However what I will say is that there are some very good standards out there. I think clearly of the ISO 27000 family which certainly within government as a whole all government departments have asserted their conformance with ISO 27001 some going slightly further than the ISO standard some remaining with the ISO controls as part of their strategic Information Assurance policies. It is an international standard so it should work equally well within the maritime environment of the UK, Singapore, United States, Canada or New Zealand.	1. Applying international standards should help joint operations and shared information environments.	72. International security standards 73. Joint operations 74. Shared information
CC Q14	The security controls within the MODUK would fully meet and exceed the ISO 27000 controls and this has been so for many years. It has been said that the ISO standard is catching up.	1. MODUK could have a role to play in devising international standards.	75. International security standards

SY1: Summary of initial analysis



SY2 24th June 2009

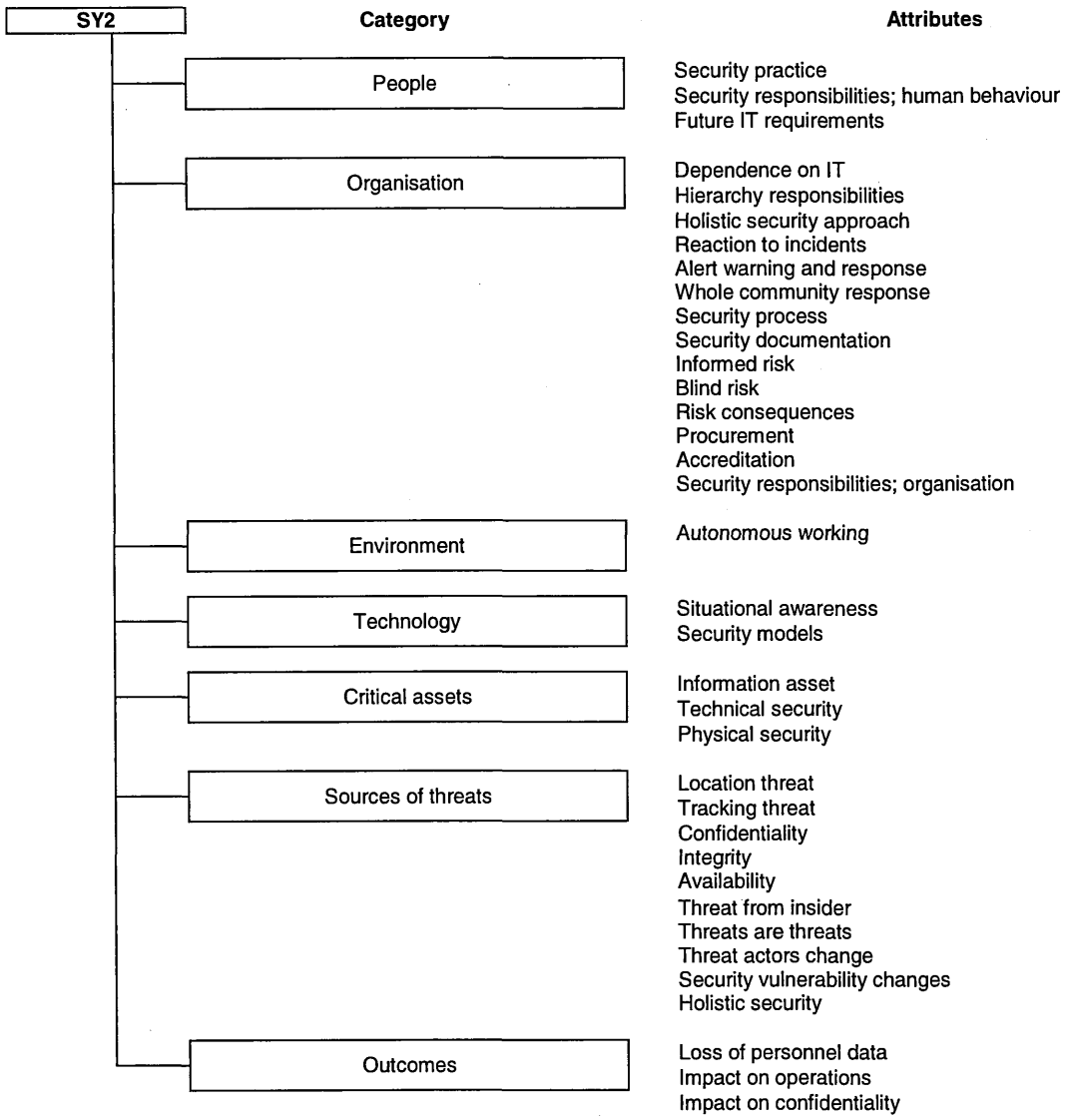
Data block and question	Interviewee's opinions of maritime environment and ICT security	Researcher's interpretation of interviewee's opinions	Research code
A Q1	Crews must be prepared for autonomous working. There is a need for ships to be able to work without links to UK or other commands.	1. In the event of IT failure	76. Autonomous working
B Q2	Technology will under pin all maritime activity and be the main deliverer of operational capability.	1. Dependence on IT	77. Dependence on IT
C Q2	For example, AIS (Automated Identification System) has security implications. AIS is similar to IFF (Identification Friend or Foe) for aircraft. Naval vessels would switch off AIS if going into an operational mode and switch on for safety. The ill-disposed can benefit from knowing position.	1. AIS intended to help situational awareness but can be used by the ill-disposed to locate and track potential targets	78. Situational awareness 79. Location threat 80. Tracking threat
D Q3	Yes, essential. IT security an enabler without which we could not rely on information to do our business.	1. Dependence on CIA	81. Confidentiality 82. Integrity 83. Availability
Q4	Omitted because SY2 still somewhat uncomfortable and so did not want to worsen the situation		
E Q5	In HMG the policies of the Chief Information officer and the Command Information Officers are moving towards exploiting information not just protecting it.	1. The need to make best use of information as an asset	84. Information asset
F Q5	A MODUK security diagram should include information exploitation leading from IT Security (ITSy) and Information Assurance should be shown as overarching the physical and technical aspects of security.	1. The hierarchy of IT security functions includes technical and physical aspects	85. Hierarchy responsibilities 86. Technical security 87. Physical security
G Q5	The perception is compartmentalised but in my opinion it should be holistic. For example, when asked, Users will say: 'The Principle Security Advisor does that', when in fact security in the round should be engrained in the culture. Security training is a cross boundaries issue.	1. Security should be viewed as a 'whole ship' activity not compartmented and then forgotten about by the majority	88. Holistic security approach
H Q6	There has been a tightening of security control. Some of the measures are off the back of the Burton and Hanigan reports in 2007/2008. The reaction to security breaches in 2007/2008 may have been inappropriate. For example, the census of removable media takes a lot of time and effort and I question the value when perhaps accounting and tracking are more important.	1. Security controls have been tightened because of the loss of personnel data and continued security breaches by the Department 2. Reaction may have been inappropriate	89. Reaction to incidents 90. Threat from insider
I Q7	Loss of intelligence feed in the middle of a sensitive operation could lead to operational compromise. We use Impact Table to assess potential damage. You can imagine the loss of the Nuclear Firing Chain! A full range of activities would be affected. We need confidentiality, integrity and availability to conduct our business effectively. A Protective Marking is related to national security breach. The Impact Table expands this into the loss of capability. For example the likely impact of the loss of a pay system. This underpins risk management of information.	1. Loss of information at critical situation 2. Impact tables used to assess potential damage 3. Dependence on IT 4. Protective marking for confidentiality	91. Situational awareness 92. Impact on operations 93. Impact on confidentiality

Continued ....

SY2

Data block and question	Interviewee's opinions of maritime environment and ICT security	Researcher's interpretation of interviewee's opinions	Research code
J Q8	There are no new threats but changing 'threat actors' and the associated security vulnerabilities need a more 'holistic approach' and a better understanding of security by all players.	1. No new threats 2. Changing threat actors 3. Security vulnerabilities change 4. Needs holistic security approach to cope with problems	94. Threats are threats 95. Threat actors change 96. Security vulnerability changes 97. Holistic security
K Q9	MOD CERT [Computer Emergency Response Team] issues warnings on a daily basis. We continue to be vulnerable to existing and upcoming threats. Threats are dependent on potential enemies who want to exploit the vulnerabilities. We need to take a more holistic view. Through life consideration of computer systems is for everyone. From design, delivery, operation and Users; all have a part to play.	1. How to keep the community appraised of current situation 2. Whole community required	98. Alert warning and response 99. Whole community response
L Q10	The RN and MODUK have the right security processes and practices in place but the MODUK security manual is considered to be large and unwieldy by the community that use it.	1. The right processes and practices supported by a document which is large and unwieldy	100. Security process 101. Security practice 102. Security documentation
M Q11	This depends upon perception. When you accept risk your decision is informed and effective then the answer is no. As long as the risk is accepted then again the answer is no. I suspect risk taking is ill judged. We probably take risk we do not know about. In Navy Command we have a lot of systems that we do not know about form either a systems or security perspective. Someone buys a system which presents a risk, especially if the system interfaces with other systems. Commanders buy but do not fully understand the consequences.	1. Risk based decision has to be informed to be effective 2. Risk environment not known 3. Consequences of taking security risk are not understood	103. Informed risk 104. Blind risk 105. Risk consequences
N Q12	We do not know the cumulative risk. We should be trying to match procurement to system security accreditation.	1. Procurement of IT should include security accreditation as part of the process	106. Procurement 107. Accreditation
O Q12	If I had my way we would have the service providers better understanding their roles and responsibilities. Trying to accept IT responsibility not PSyA. Systems must be fit for purpose and present acceptable risks. N6 etc. better understand their responsibilities.	1. Service providers do not understand their responsibilities 2. RN Divisions do not understand their responsibilities	108. Security responsibilities; organisation 109. Security responsibilities; human behaviour
P Q12	Scenario – I need a computer in that tent in 12 hours but cannot accredit. But, to deliver in future with knowledgebase and understanding then security culture needs to be engrained within the delivery organisation. There has been a top down directive to IPTs. Should apply to N6 ISS deliverers but not resourced.	1. Predict the requirement and then have a solution ready to go	110. Future IT requirements
O Q12	The Maturity Model is focused on Protect [This is a new Protective Marking]. If that is the requirement then good. If the security process is to cover more, then the model has to be expanded. But generally it does what it needs to and well thought out. It is questionnaire focused direct at MODUK level. At TLB level it is open to interpretation.	1. IAMM is fit for purpose	111. Security models
Q13 to Q17 inclusive	Omitted because of time constraint		

SY2: Summary of initial analysis



SY3 8th July 2009

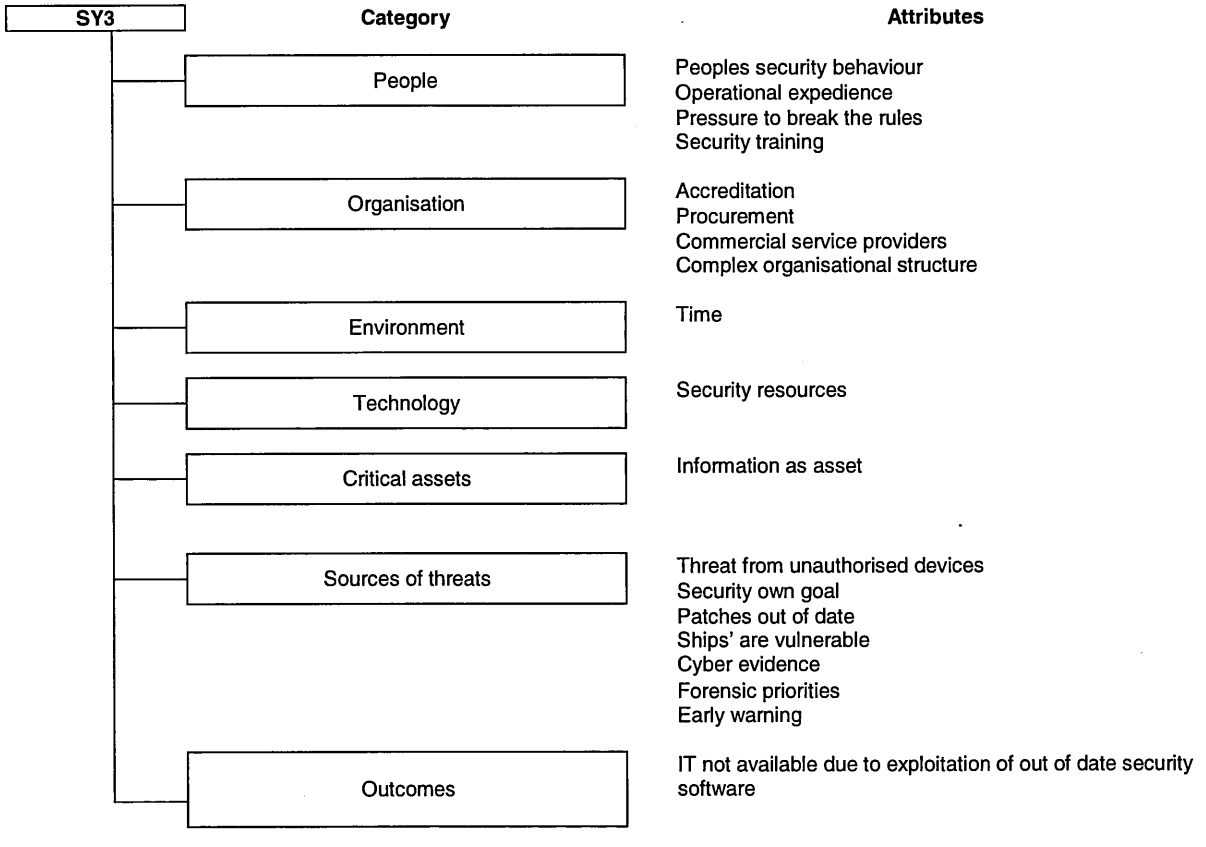
Author's note: SY3's wife was ill and arrived at the interview in somewhat of a distracted state. He was offered the opportunity to re-schedule the interview but he declined stating that he would rather work to keep his mind off the problem. This interview started with Q1, but was allowed to stray off track. Even so, good data was generated during the shortened interview.

Data block and question	Interviewee's opinions of ICT security in a maritime environment	Researcher's interpretation of interviewee's opinions	Research code
A Q1	The difficulty in any environment is Users not following accreditation rules. If they read and adhere to Security Operating (SyOps) instructions then I would be out of work.	1. Not following the security rules	112. Accreditation 113. Peoples security behaviour
B	Users circumvent the rules. For example, and the rules state that only MODUK authorised [crypto enabled] data pens can be used with MODUK systems and that these data pens must not be used on any other system [say, a private laptop]. So, if a member of staff is under pressure to finish work and this can only be done at home, and then they will break this rule	1. Circumvent rules 2. Threat from unauthorised memory and other devices 3. Pressure of work leads staff to take short cuts	114. Peoples security behaviour 115. Threat from unauthorised devices
C	Rules are also overridden in urgent operational circumstances, for example' the transfer of information between international partners.	1. Security acknowledges the need for operational expedience.	116. Operational expedience
D	In a military environment (I am not sure about civilian procedures) our procedure [procurement] is not aligned with IT security. A commanding officer can demand an urgent operational requirement via an Integrated Project Team (IPT) and the IPT can deliver and so circumvent accreditation issues. When the IT Security Officer (ITSO) is the also the Deputy Weapons Electrical Officer (DWEO) needs to make his mark, then if the CO wants something then the DWEO won't say no. If the DWEO is doing his job supporting MODUK not CO then the procedure is aligned to accreditation.	1. Procurement and security requirements are not aligned 2. Accreditation issues 3. Conflict of loyalty to Commanding Officer or security	117. Procurement 118. Accreditation 119. Pressure to break the rules
E	Communications security processes are generally considered to be good, but even here Users often break the rules.	1. Security process is good but people break the rules	120. Peoples security behaviour
F	I do not think training is the problem.	1. Security training is not a problem	121. Security training
G	The ability to get anti-virus and patches to units is a problem. MODUK policy does not allow certain types of file extensions to be used over the network. This means that patches have to be mailed to ships and so can be out of date before being applied.	1. Security rules prevent certain file extensions being used. For example .zip files are not allowed. Patches are burned onto CDs and posted to ships.	122. Security own goal 123. Patches out of date 124. Ships' are vulnerable

Continued ....

Data block and question	Interviewee's opinions of maritime environment and ICT security	Researcher's interpretation of interviewee's opinions	Research code
H	There is a 'disconnect' between what the military security organisation needs and the commercial service provider delivers. It has been known for [ICT] service providers to destroy cyber evidence because their priority is to restore the service not maintain forensic evidence. For example, if a User discovers a virus and inform Atlas [the consortium that provide equipment and technical support] then they [Atlas] will clean up the system and close the incident. This destroys evidence, and solves nothing – the originator of the virus is still at large.	1. Commercial service providers put commercial considerations before MODUK security process. 2. Cyber evidence 3. Different forensic priorities	125. Commercial service providers 126. Cyber evidence 127. Forensic priorities
I	We send Fleet Situational Awareness Notices ahead of MODUK Computer Emergency Response Team and the Joint Security Co-ordination Centre – we try to be proactive.	1. Attempt to stay ahead by issuing early warning	128. Early warning
J	This organisation [WARP] deals with Information Systems. Another RN organisation deals with compliance checking, and then there are RN physical security teams.	1. Complex security organisation within Royal Navy	129. Complex organisational structure
K	Information is one of the most important assets after the individual. We spend a lot of time and resources protecting our information.	1. Information as asset 2. Time and resources used	130. Information as asset 131. Time 132. Security resources

SY3: Summary of initial analysis



INT1 23rd June 2009

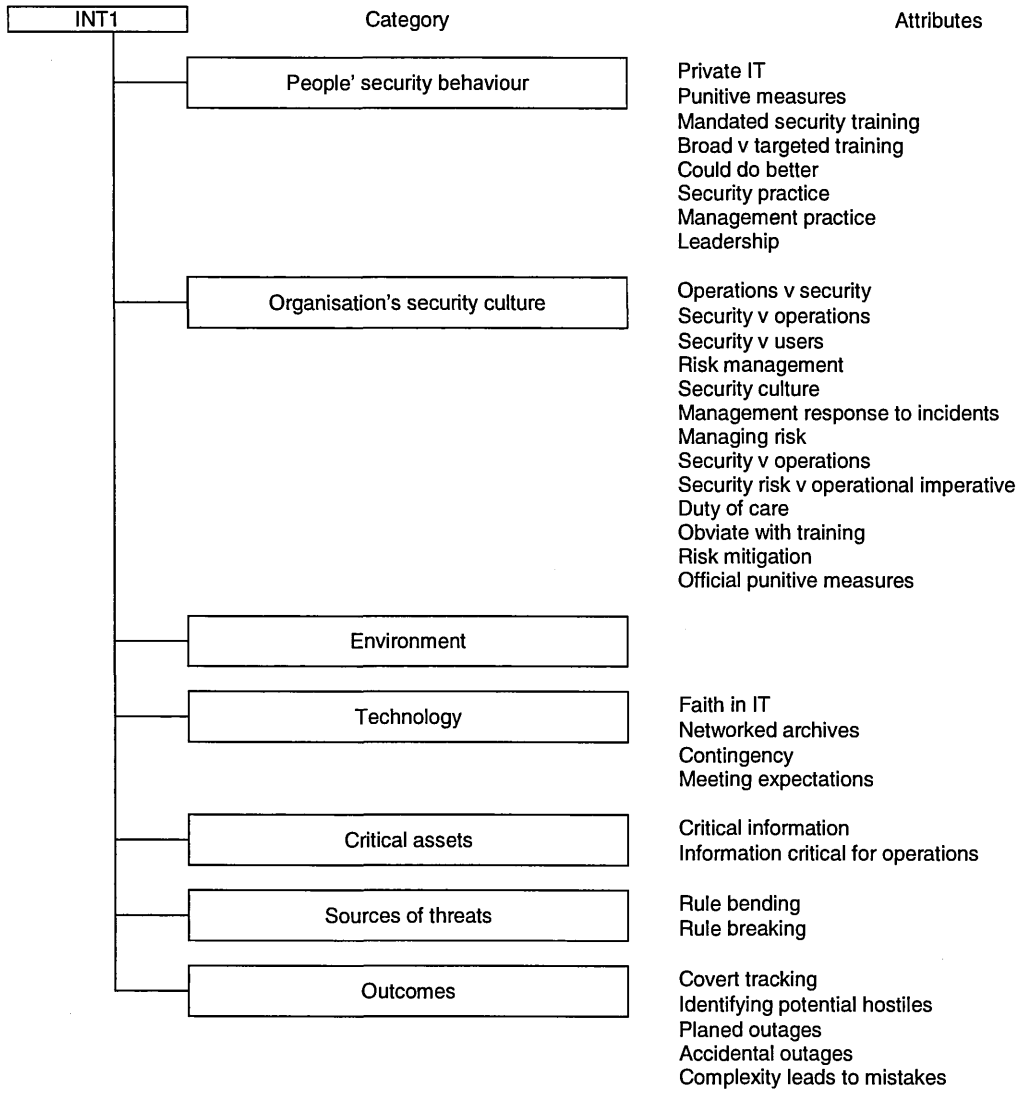
Data block and question	Interviewee's opinions of ICT security in a maritime environment	Researcher's interpretation of interviewee's opinions	Research code
A Q1	At sea the operational imperative takes precedence. For example I recently headed a team working in six separate domains. Each domain represented one country with different technical standards and operating procedures. Ashore we follow the rules, but work afloat requires an ability to conduct risk management. If the IT is insufficient, for example different networks, unconnected standalones and the need to use private IT then that can lead to 'bending of the rules'. In such cases we remain accountable for our actions and therefore a level of self-risk assessment is called for. There is also a need to protect juniors from actions which could put them at risk of disciplinary action.	1. Afloat, operations take precedence over security 2. International information exchange 3. Multiple international technical standards 4. Ashore, security takes precedence over operations 5. Afloat risk balance between operations and security 6. Plethora of IT 7. The need to use private equipment – rule bending 8. Subordinates need protecting from punitive consequences of rule bending	133. Operations v security 134. Security v operations 135. Risk management 136. Private IT 137. Rule bending 138. Punitive measures
B Q2	The Automated Identification System 'Blue Picture' is an important element. It helps build the intelligence picture and allows naval units to prosecute contacts that are not squawking an official code.	1. Own IT working against us 2. Vessel not transmitting AIS would be worth investigating	139. Covert tracking 140. Identifying potential hostiles
C Q3	Critical. I support the activities of the CIO. He is responsible for ensuring Information Assurance, security compliance and best practice.	1. Information is business and operationally critical	141. Critical information
D Q3	I recently completed an Information Security course which is now mandated for all MODUK personnel. It was intuitive. However, I feel that those with less experience may not get as much form the content.	1. Security training mandated following incidents involving the loss of personal data 2. One size training does not necessarily fit all	142. Mandated security training 143. Broad v targeted training
Q4	Wanted to move on so because sufficient time spent on Q1 to Q3.		
E Q5	Yes, but protecting our information could be better. Having worked with the Americans they seem to have a better understanding of IA. In the RN there can be a disconnect between Users awareness and experts requirements. Memory sticks for example have been used widely which is against security policy. However, if User needs to transfer data between systems then 'data sticks' are used. That was until a recent crackdown following the personal data losses. It is also important for Users to be able to trust the archiving mechanisms. Work is underway to improve the RN [electronic] archive.	1. Could do better 2. Security experts have expectations that users cannot always reach 3. Rule breaking 4. Electronic archiving does not have a good reputation in the RN. Users have been known to burn documents etc. to CD and keep in filing cabinet. This breaches the Freedom of Information Act.	144. Could do better 145. Security v users 146. Rule breaking 147. Faith in IT 148. Networked archives
F Q6	Yes, HMG are trying to rework known and trusted methodology when a simple fix would probably have done.	1. IAMM is an over reaction	149. Management response to incidents
G Q7	This happens today on a regular basis and can be caused by anything from a crypto change over to technicians going off for a cup of tea. In these situations life stops. This is because operations and life on-board ship are organised around IT.	1. Planed outages 2. Accidental outages 3. Information critical for operations	150. Planed outages 151. Accidental outages 152. Information critical for operations

Continued ....

INT1

Data block and question	Interviewee's opinions of maritime environment and ICT security	Researcher's interpretation of interviewee's opinions	Research code
H Q8	Yes, [international] Operation Atalanta is run in an unclassified environment. However, UK information and intelligence from the HQ at Northwood will have much higher protective markings. Therefore we (UK) have to be careful in vetting what we release. There are certain rules governing sensitive information which can be broken in extremis and at a Commanding Officers' discretion. However, this 'Action on' has to be justified to the Director GCHQ.	1. The plethora of IT and information needed for international operations can lead to mistakes 2. Information exchange rules can be broken it special circumstances but such actions have to be justified to higher authority	153. Complexity leads to mistakes 154. Managing risk
Q9	INT1 did not want to talk about this subject		
I Q10	Yes. Plans are in place to try and improve the situation.	1. Lax security practice can cause incidents	155. Security practice
J Q10	Again, this comes down to the operational imperative. We are trained not to break the rules. But obeying the rules and doing the job right takes time. Therefore there has to be value judgement. Constant look out for bad practice. Difficult to interpret and so protect others information. Mitigation includes training, management and leadership.	1. Following security rules can lead to operational difficulties 2. Balance between security risk and operational imperative 3. Need to protect other nationalities information 4. Difficulties with bad practice obviated by training, management and leadership	156. Security v operations 157. Security risk v operational imperative 158. Duty of care 159. Obviate with training 160. Management practice 161. Leadership
K Q11	We must sign up to accept that things will go wrong. We can disguise information to mitigate risk. To protect the information we must understand the overall picture. Improving information culture.	1. Need contingency plans 2. Risk mitigation 3. Must understand the operating environment 4. Information culture	162. Contingency 163. Risk mitigation 164. Environment 165. Information culture
Q12	INT1 did not want to talk about this subject		
L Q13	If Americans detect irregularities they cut links between systems. This can be counterproductive. We could be more surgical with new technology.	1. Immediate action – cut links 2. Lose chance for intelligence gathering	166. Contingency 167. Intelligence gathering
M Q14	The growing expectations for IT are not always being met. In general, in the Services we deal, live and breathe security.	1. IT not always living up to expectations 2. Security culture	168. Meeting expectations 169. Security culture
N Q14	We have the Official Secrets Act as the ultimate sanction.	1. Official punitive measures	170. Official punitive measures
Q15, Q16 and Q17	Omitted due to time constraint		

INT1: Summary of initial analysis

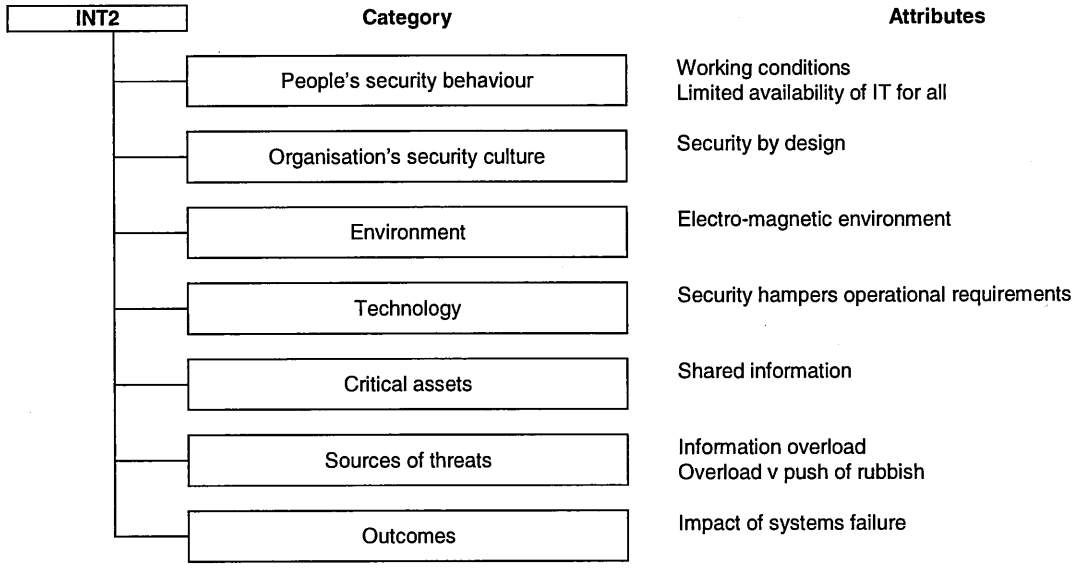


INT2 23rd July

Author's note: The interviewee was pressed for time which resulted in a rushed interview and less depth (30 minutes). The result was an informal discussion where the following points were made:

Data block and question	Interviewee's opinions of ICT security in a maritime environment	Researcher's interpretation of interviewee's opinions	Research code
A Q1	Yes it does: issues with bandwidth; office space; routines and access to IT. For example, juniors have to queue to get on the system.	1. Space in the electromagnetic environment at a premium 2. Limited working space on-board 3. Limited IT available for crew	171. Electro-magnetic environment 172. Working conditions 173. Limited availability of IT for all
B Q2	In fight environment well provisioned. We also use IT for 'Medicare'. All with bandwidth issues.	1. Also use IT to collect information from external sources	174. Shared information
C Q3	Serious potential that we cannot get information we need to sea. Need to be disciplined to do it. There is not an information overload – but people pushing rubbish which is a disabler.	1. System failure prevents flow of information needed to conduct operations. 2. Not an information overload, just people pushing rubbish which clogs the system	175. Impact of systems failure 176. Information overload 177. Overload v push of rubbish
	At this stage it appeared that the INT2 was becoming deeply uncomfortable. He was offered the opportunity to end the interview but he wanted to continue. Rather than make the situation worse, the researcher set the questions to one side. The remainder of the time was spent in informal conversation during which INT2 raised the following points:		
D	I find I am returning to more traditional ways of working due to a combination of factors.	1. Cannot make system work so returning to e-mails with attachments.	178. Security by design
E	We are IT inhibited, many people that we work with in this building, they cannot access MODUK systems so cannot use links etc.	1. Connectivity to all parts of the organisation not in place so 'web working' not always possible	179. Security hampers operational requirements
F	The C to F [Defence Information Infrastructure] migration was a step back in capability. I spend 30 minutes per day managing e-mail rather than issues.	1. Migration to new system was not well managed and was seen by some as a backward step.	180. Security by design

INT2: Summary of initial analysis



ENG1 6th July 2009

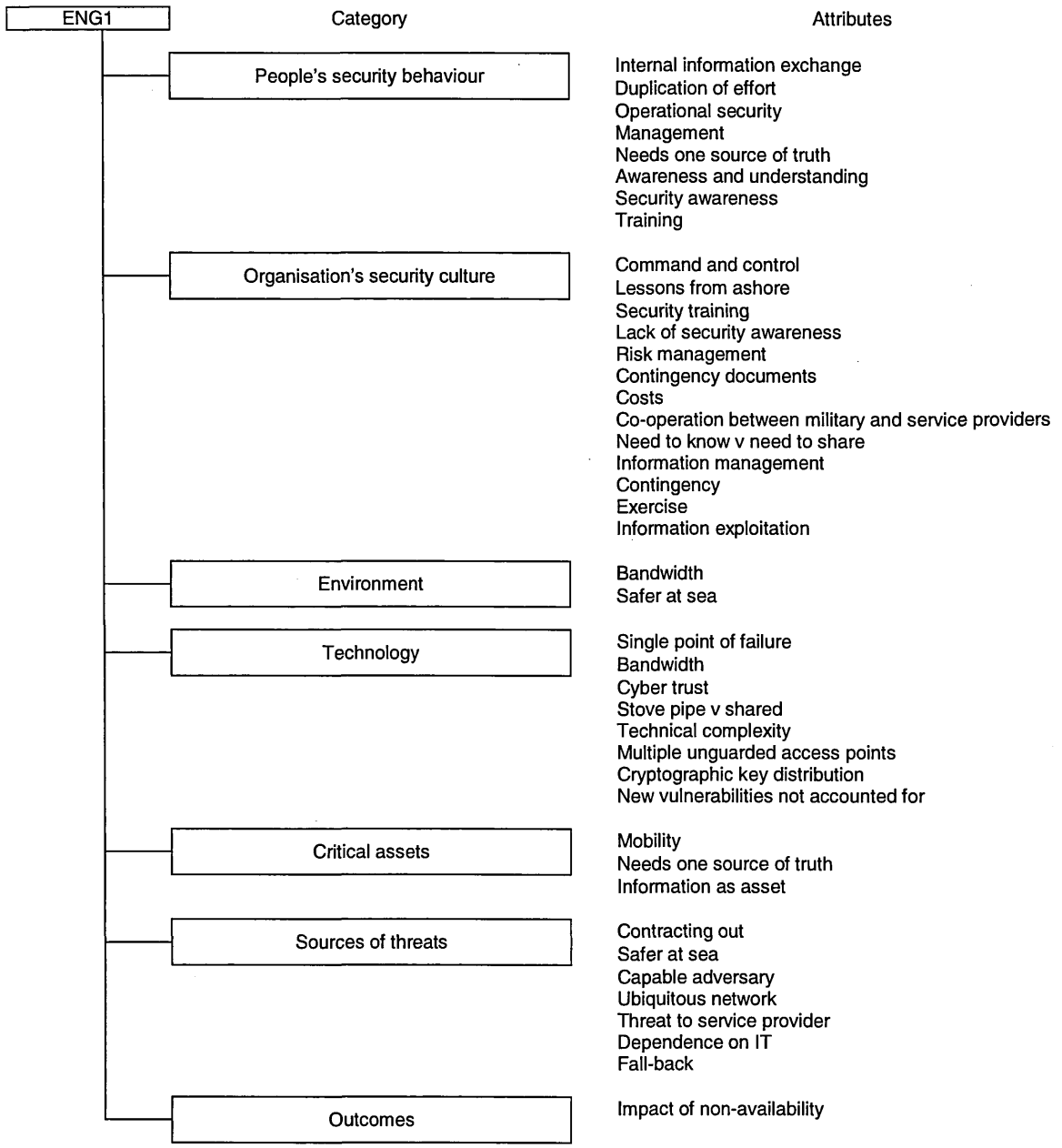
Data block and question	Interviewee's opinions of ICT security in a maritime environment	Researcher's interpretation of interviewee's opinions	Research code
A Q1	Yes it does. You have the element of bandwidth which makes it more difficult. Other environments are similar: mobile environments. We have a paucity of communications connectivity.	1. Restrictions due to bandwidth 2. Similar restrictions apply in land environment 3. Limited communications options	181. Bandwidth 182. Mobility 183. Single point of failure
B Q2	We spend more time sitting on e-mail. Unfortunately systems are still stove piped. Organisation boundaries within single platform [chain of command] require communications using e-mail with little automation [no web working]. This means our on-board information exchange is poor. We still have to make sure our paper BRs are up to date and correct.	1. Intelligence, management, warfare etc. all on their own system 2. Self-imposed network restrictions 3. Duplication of effort (Paper and electronic books) 4. In case on-board systems fails	184. Stove pipe v shared 185. Command and control 186. Internal information exchange 187. Duplication of effort 188. Contingency documents
C Q3	Enormously. From a communications point of view [IT] is very important, but lots of underlying support activity is not done well.	1. Important for operations 2. Support activity	189. Operational security
D Q3	Operations stuff is weighed off [well done] but the support side absolutely terrible. For example, making reports and returns.	1. Reports and returns	190. Management
E Q3	How the information is held, including spread sheets; there is no compatibility and different formats. It is the same information but people busy reformatting. The information should be available – most tools are geared up to top level management. As such, the resultant information is no use to Users.	1. Time wasted reformatting to satisfy different parts of the same organisation	191. Needs one source of truth
F Q4	Haphazard, haphazard and haphazard; I refer back to my previous answer!	1. Haphazard 2. Haphazard 3. Haphazard	192. Information management 193. Information exploitation
G Q5	Information is an important asset, but it depends on which level of the organisation you talk about. At higher levels it is very important; lower down not cognisant of what information means. People are not trained	1. Information is an asset 2. Awareness of information as an asset varies across the organisation	194. Information as asset 195. Awareness
H Q6	There has been a bit of a shift. IA, in my view, completely focused on not getting it – the need to know. Showing signs of making sure getting it – the need to share. Poor on making sure information accurate and correct. Big factor of not managing it well.	1. Returned to an earlier paradigm, need to know, because of data losses 2. Starting to settle back into need to share 3. Issues with information management	196. Need to know v need to share 197. Information management
I Q7	As it stands from a support point of view and the way they operate or organised – if IT stops then everything stops. Ships don't sail, helicopters don't fly. IA processes should have allowed continuity – having the right fall-backs – but we have lost the knack. IA is ignored, not trained, not exercised.	1. IT critical for all operations 2. Lack of fall-back capability 3. Lack of contingency plans 4. Lack of IA awareness and understanding 5. Lack of training 6. RN does not practice for working without IT	198. Dependence on IT 199. Fall-back 200. Contingency 201. Awareness and understanding 202. Training 203. Exercise
J Q8	MT WAN etc. will give more access points and lead to more complexity. Difficult to co-ordinate encryption key handling. IP crypto may help. In a maritime environment [IP crypto] by 2012 perhaps further.	1. Greater complexity of connections and poor working practice will worsen the situation 2. Traditional cryptographic methods too expensive and complex for international network working	204. Technical complexity 205. Multiple unguarded access points 206. Key distribution
K Q8	Complete integration into DII. You cannot use it for what you need it for. New vulnerabilities to Centre. Single point of failure.	1. Ubiquitous network 2. Impact of non-availability 3. New vulnerabilities not accounted for 4. Single point of failure	207. Ubiquitous network 208. Impact of non-availability 209. New vulnerabilities not accounted for 210. Single point of failure

Continued ....

ENG1

Data block and question	Interviewee's opinions of maritime environment and ICT security	Researcher's interpretation of interviewee's opinions	Research code
Q9	Omitted because of time constraint		
L Q10	Yes, training is a huge issue. We are trying to improve.	1. Issues with security training 2. Plans in place to improve	211. Security training
M Q10	The other problem is without knowledge of security there is little control. For example, to improve welfare connectivity a local Internet Service Provider (ISP) was used to set up a 'hot spot' on board a ship. This shows a lack of understanding at the command level'	1. Lack of awareness of security issues and likely outcomes of incidents	212. Lack of security awareness
N Q11	So difficult and linked to previous answer. Without training and understanding you have to lock down which stops business. Risk – with a lack of understanding you cannot take risks.	1. Link between security awareness and risk management	213. Lack of security awareness 214. Risk management
Q12, Q13 and Q14	Omitted because of time constraint		
O Q15	They must be a bit different. It depends; I would expect physical security would be better and in electronic environment as well. An attack would be fairly expensive so you would need to be a capable adversary. More likely to look for a cheaper option.	1. At sea, likely that physical and virtual environments safer 2. Too expensive to attack 3. Would require capable adversary 4. Adversary would look for cheaper option	215. Safer at sea 216. Capable adversary
P Q16	There seems to be an appetite to move towards commercial services and virtual private networks. This forces costs down but will change the threat. Sharing communications networks with commercial increases the threat.	1. Contracting out network and other services 2. Reduces costs 3. Changes threat 4. Network shared with commercial organisations	217. Contracting out 218. Costs 219. Changes threat 220. Changes vulnerability
Q Q16	Could lead to denial of service if this becomes primary means. We would defend the traffic but not the service provider. We are not training or exercising this scenario [denied civil communications].	1. Network provider lies outside the 'umbrella' of military protection 2. Traffic stream may be encrypted but what if service provide under attack? 3. Lack of understanding of this problem	221. Threat to service provider 222. Co-operation between military and service providers
R Q17	Yes, probably can use commercial methodologies although there are nuances and slight differences. Availability of bandwidth connectivity which limits how well you can assure your information. We have a resynchronisation and trust requirements – is this the entity you want to talk to?	1. Lessons from land environment could be applied afloat 2. Bandwidth restrictions apply to security 3. Establishing cyber trust	223. Lessons from ashore 224. Bandwidth 225. Cyber trust

ENG1: Summary of initial analysis

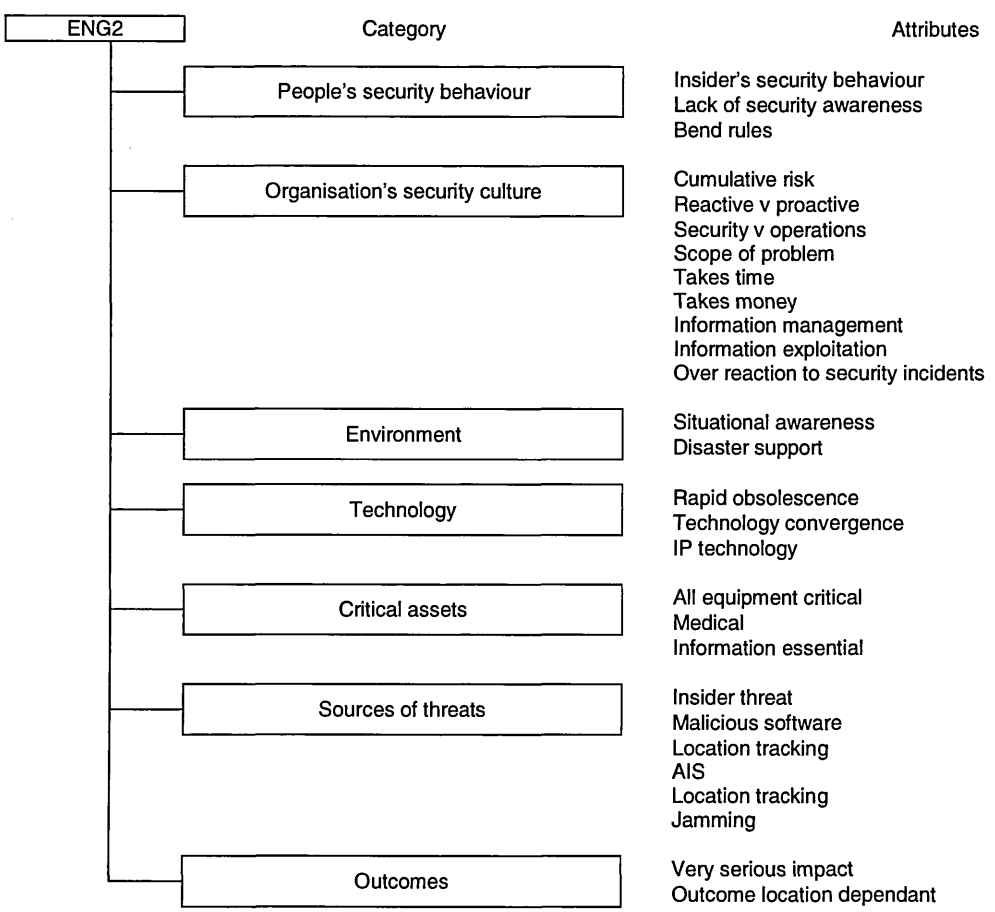


ENG2 24th June 2009

Data block and question	Interviewee's opinions of ICT security in a maritime environment	Researcher's interpretation of interviewee's opinions	Research code
A Q1	It is different but getting closer in that technology available ashore is now more accessible on ships.	1. Technology convergence	226. Technology convergence
B Q2	For example, in 1984 in the Falklands I could make an HF radio telephone call to talk to my wife. In 2004 In HMS Invincible, I could ring direct, browse the internet and watch satellite TV in my cabin.	1. IP voice and data services now permit communications which are similar to those available in the land environment	227. IP technology
C Q3	Commercial gain can be obtained from knowing where your competitor's ships are. I understand that certain commercial companies are turning off their AIS. This is allowed in high threat areas.	1. Location tracking used by the ill-disposed to gain advantage 2. Rules can be held in abeyance in high threat areas	228. AIS 229. Security v operations
D Q3	Access to the Internet helps in disaster relief. For example, unclassified satellite pictures of earthquakes are used to help understand a situation. AIS will identify what ship is where and give an INMARSAT number if fitted.	1. Access to Internet technology helps military vessels to take part in relief operations involving government and commercial organisations	230. Location tracking 231. Disaster support
E Q3	In 2005 an RN helicopter ditched in the Gulf. We were not close but we were able to use AIS and INMARSAT to coordinate the rescue using AIS data.	1. An example of commercial location tracking used to help military operation	232. Location tracking
F Q3	Telemedicine is now more robust and we make regular reports to the Met office. This may be automatic.	1. Medical emergencies 2. Weather reports	233. Medical 234. Situational awareness
Q4	Omitted because of time overrun on Q3		
G Q5	Information as an asset is essential, from running an organisation through to battle winning advantage.	1. Information essential across all parts of an organisations to enable its activities	235. Information essential
H Q5	We are trying to get our arms around it. Information management is hugely difficult, time consuming and expensive. We are moving into IM but not necessarily achieving information exploitation.	1. Scope of the problem not fully understood 2. Time consuming and expensive 3. Getting better at information management but not how to put information to good use	236. Scope of problem 237. Takes time 238. Takes money 239. Information management 240. Information exploitation
I Q6	The information assurance problem area was relatively small. The Burton and Hannigan reports cover everything, and we trying to do all recommendations at once. This will take a lot of time and effort to make successful.	1. Sledge hammer to crack a walnut 2. Time consuming 3. Lot of effort required	241. Over-reaction 242. Takes time 243. Takes effort
J Q7	Very serious impact. At worst huge impact on UK and world economy. You can think of a big merchant ship losing communications may not be so serious – losing control of machinery mid Atlantic? An EM [electromagnetic] pulse could lead to economic meltdown. It is possible to jam GPS [Global Position System] satellites and these satellites are due to fall out of the sky in 10 years.	1. Very serious impact across the world 2. Outcome location dependant 3. GPS jamming	244. Very serious impact 245. Outcome location dependant 246. Jamming 247. Situational awareness
Q8	Covered in by response to Q7		
K Q9	We use firewalls shore side. Seen from a Merchant Navy perspective even with firewalls what happens when the Chief Engineer downloads a virus which stops the ship.	1. Technical solutions shore side can be transparent to users. However, when afloat the same transparency may not be possible	248. Insider threat

Data block and question	Interviewee's opinions of ICT security in a maritime environment	Researcher's interpretation of interviewee's opinions	Research code
L Q10	A major cause. People told not to put dongle into machines but it still happens. There have been examples where ship's staff have upload virus using their own memory devices. There is a lack of understanding and training which leads to this sort of thing.	1. Users use un-authorised IT in official equipment. 2. Accidental or deliberate uploading of malicious software 3. Lack of security awareness	249. Insider threat 250. Malicious software 251. Lack of security awareness
M Q11	At sea you do what you need to do. Although we have non-operational systems at sea they can be critical. Shore side can afford to be less resilient. Potentially accepting cumulative risk is increasing our vulnerability.	1. May have to bend the rules 2. Even IT which may not be considered as critical has a role to play 3. Cumulative risk is a bad idea	252. Bend rules 253. All equipment critical 254. Cumulative risk
N Q12	Potentially risk on risk increasing vulnerability.	1. Cumulative risk increasing vulnerability	255. Cumulative risk
Q13 and Q14	Omitted because of time constraint		
O Q15	We are always playing catch up with technology; it is difficult to play catch up because of the rate of change. Simon Singh talks about this in his book [The Code Book].	1. IT tends towards rapid obsolesce 2. Tend to react rather than being pro-active	256. Rapid obsolescence 257. Reactive 258. Proactive
Q16 and Q17	Omitted because of time constraint		

ENG2: Summary of initial analysis



ENG3 7th July 2009

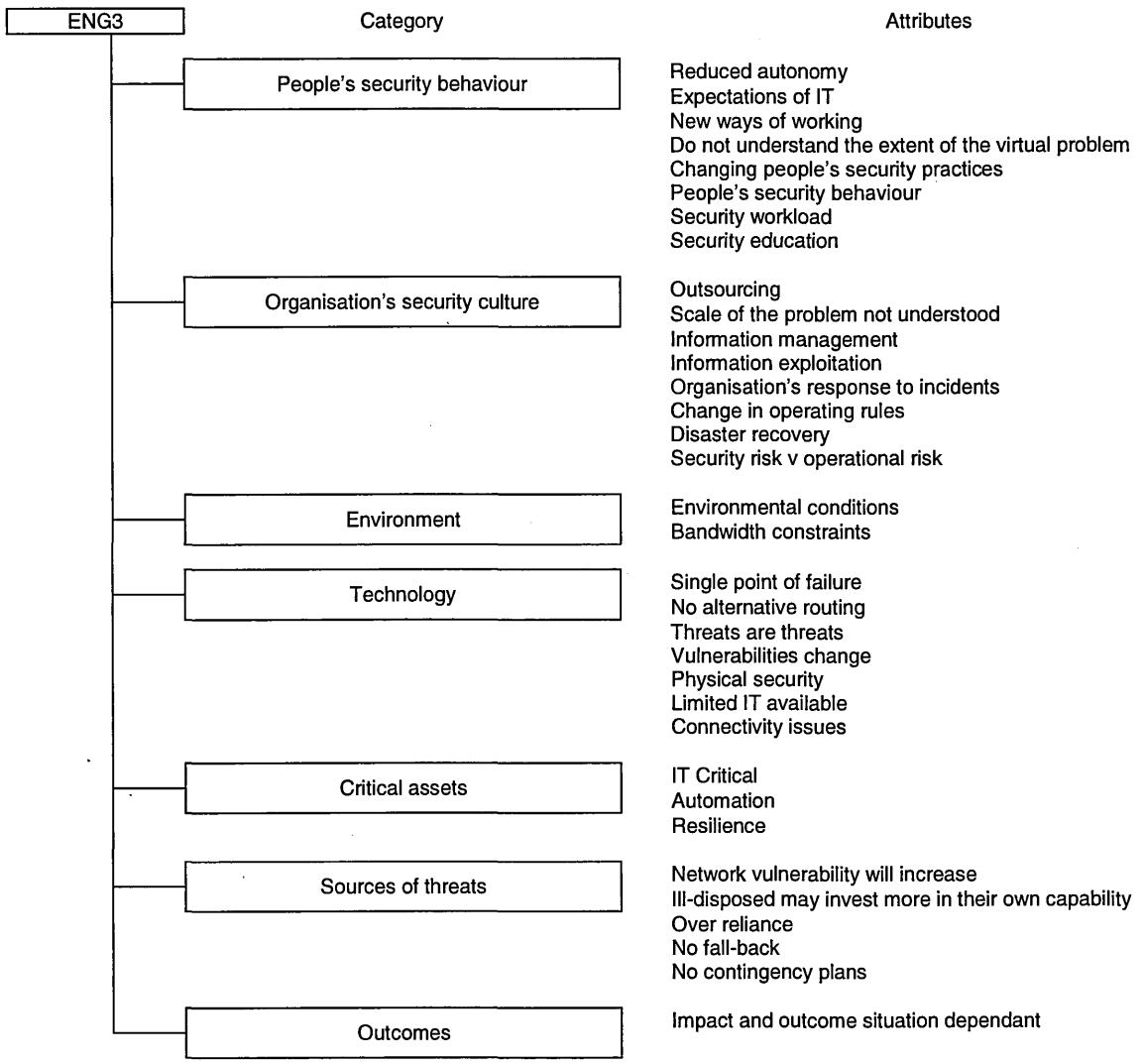
Data block and question	Interviewee's opinions of ICT security in a maritime environment	Researcher's interpretation of interviewee's opinions	Research code
A Q1	Yes it does. The challenges are the independent nature of a maritime unit and connectivity. For example, submarines and the intermittent nature of that connectivity. In terms of information assurance I am not sure if it is different working in an office or in a ship. Information assurance applies across the board. Connectivity and bandwidth restrict use.	1. Ship's crews have been used to a high level of autonomy once away from shore. 2. New technology reduces this autonomy to a certain extent 3. Submarines still display some of the characteristics of pre-broadband due to their operating environment 4. Even so, limited IT and bandwidth still cause issues	259. Change in operating rules 260. Reduced autonomy 261. Environmental conditions 262. Limited IT available 263. Bandwidth constraints
B Q2	Using it more now than when I was last at sea. I think contacting land or civilian environment will not have changed as much as you would expect. More sophisticated than in the past but not as significantly as in other areas due to constraints – bandwidth and connectivity. There is a greater use of data transmission compared to several years ago.	1. More use on-board because of improved capability 2. Ship to shore connectivity still an issue 3. More use being made of IP data connections	264. Expectations of IT 265. Connectivity issues 266. New ways of working
C Q3	To a large extent it is critical to maritime activity in both non-military and military contexts. Not least by the nature of the technology available to the RN. Ultimately, using technology will become smarter and potentially reduce the number of units to achieve the same effect. This could apply to wider maritime, for example deep sea fishing.	1. IT critical 2. Automation needs fewer units to achieve the same aim	267. IT Critical 268. Automation
D Q4	RN information management is inefficient with too much none-targeted information. The information management organisation on-board is undergoing re-organisation ahead of Information Assurance Maturity Model, which is HMG's response to the data loses in 2007/2008.	1. Inefficient 2. Non targeted information means push everything and hope something sticks	269. Information management 270. Information exploitation
E Q5	Viewed from hierarchy perspective then going that way; taking organisation as a whole then not so much.	1. Senior management starting to 2. Overall, not so much	271. Information management 272. Changing people's security practices
F Q6	Well, the establishment of the MODUK Chief Information Officer (CIO) and the re-brigading of the Director General Information (DGInfo) suggest hierarchy are trying to take information seriously. For the RN, the designation of DCinC as CIO suggests the same. Also SIO is now the senior risk owner.	1. Reorganisation of responsibilities following security incidents	273. Organisation's response to incidents
G Q6	For on-board governance, the First Lieutenant (XO) is now the SIO. He was the Unit Security officer (USO) under the old security regime. This change is happening ahead of IAMM changes.	1. Reorganisation of responsibilities following security incidents	274. Organisation's response to incidents
H Q7	There is potential to downgrade our capability significantly risk over reliance [on new technology]. We have legacy fall-back to signal traffic that we won't have in future. Some ways we work now were not allowed in the past [joint operations]. This is situation dependant for example, if you are acting as a private ship, as part of a task force or on joint operations such as anti-piracy. Increasingly, the impact will become more severe as more dependence and will depend on folding in command systems and data link pictures.	1. Over reliance on IT increase vulnerability. 2. No fall-back 3. Dependency depends upon prevailing conditions and circumstances 4. Impact and outcome will be more severe	275. Over reliance 276. No fall-back 277. No contingency plans 278. Impact and outcome situation dependant

Continued ....

ENG3

Data block and question	Interviewee's opinions of maritime environment and ICT security	Researcher's interpretation of interviewee's opinions	Research code
I Q8	Only by virtue of the growth in the use. The IA age there is more ability to do network attack. It's worth enemy investing in attack capability. As we advance we try to address were we can. Possibly architecture having a clear blue print for the connections. Not having full handle so need to map the architecture and subsequently configure.	1. Network vulnerability will increase 2. Ill-disposed may invest more in their own capability 3. Do not understand the extent of the virtual problem	279. Network vulnerability will increase 280. Ill-disposed may invest more in their own capability 281. Do not understand the extent of the virtual problem
J Q9	The MODUK does not have a map of IT architecture being deployed and this makes management and defence of the networks inefficient.	1. Scale of problem not understood	282. Scale of problem not understood
K Q9	I am not sighted on MODUK disaster recovery. In the RN we use 'belt and braces' to make resilience. So we do not plan for recovery. A [civilian] business model would not invest in that way but would have more disaster recovery planning'. We float move fight the information system.	1. RN plan to avoid the need for disaster recovery by using massive resilience.	283. Disaster recovery 284. Resilience
L Q9	In submarines everything is about resilience. The trade-off is between safe and exploit.	1. Resilience	285. Resilience
M Q9	Stove pipe could lose the war. Timeliness of information is critical - it is more important to get the information and accept the risk. There has to be compromise.	1. Security risk v operational risk 2. Compromise between the two	286. Security risk v operational risk 287. Compromise
N Q10	Not entirely sure it is. Carelessness is simpler [easier] than security. The loss of information is due to carelessness and the lack of appreciation just how easy it is to lose information. For example, compare a 'memory stick' to an office full of files.	1. It is easier to take short cuts than it is to spend time applying security principles 2. A memory device can hold a library full of information. In the old days you would have had to break into an office and open a filing cabinet to have access to a small fraction of the information.	288. Education may be ok 289. People's security behaviour 290. Virtual data composite 291. Scale of the problem
O Q11	We will be seeing responsibility pushed down to lower levels. CO and XO will carry more responsibility. That's the way the IA is being focused. Directing risk management policy and enacting at lower levels leading to more work for individuals. The situation could be mitigated by the single Defence infrastructure; reduce having to move things about.	1. Increased security responsibility leads to more work for all	292. Security workload
Q12	Omitted because ENG3 not sited on the topic		
P Q13 and Q14	There are software tools such as sanctuary software (tie down). Utilise technology to implement policy – take the burden off individuals.	1. Make better use of security software to reduce work load	293. Security workload
Q Q15	Increasing reliance on commercial services such as Airwaves; the possibility of 'Jamming'; single points of failure; and the limited number of satellites; in a land environment you have alternative paths.	1. Reliance on outsourcing 2. Single point of failure 3. No alternative connectivity	294. Outsourcing 295. Single point of failure 296. Alternative routing
R Q15	A ship has a certain security that land environments don't have.	1. Physically secure box at sea	297. Physical security
S Q16	The spread of network capability means threat not new – threats increase. Enemy looks for vulnerabilities particularly in terms of unclassified systems.	1. Threats not new 2. Ill-disposed probe for vulnerabilities which do change	298. Threats are threats 299. Vulnerabilities change
Q17	Omitted because of time constraints		

ENG3: Summary of initial analysis



ENG4 6th July 2009

Data block and question	Interviewee's opinions of ICT security in a maritime environment	Researcher's interpretation of interviewee's opinions	Research code
A Q1	There are a lot of different challenges not seen alongside. We have long deployments and limited communications. Obtaining information to keep the business informed can be difficult at times. It is a unique environment. The working patterns are irregular. For example, you can be working full on and then alongside with little time off. Exercises present problems of endurance. We have long days at sea. As a Weapons Electrical Officer I could be up at 0800 and not finish until 2300. It's not friendly – noise and so on.	1. Peoples working conditions away from home for extended periods 2. Limited connectivity 3. Irregular working patterns 4. Exercise to extremes to test and maintain operational capability 5. Noisy environment	300. Working conditions 301. Limits with IT connectivity 302. Irregular working patterns 303. Extreme operational exercises 304. Noisy conditions
B Q2	The bulk of routine business is conducted on IT. We no longer use physical communications. For example, in this job I have had one written letter and this represents what has happened at sea. Since late 90s we have used attachments or even just text in e-mails. Information is only on line.	1. Depend on IT for routine business	305. Dependence on IT
C Q2	Many reference documents are easier to get to. The electronic versions are more up to date. The physical distribution services are now gone. So, many publications are not available. The whole (RN) world is centred on information systems.	1. Electronic reference material only 2. Not always available 3. Physical distribution stopped which means local paper copies have to be produced and kept up to date.	306. Electronic reference material 307. Updates 308. Paper backup
D Q3	As above; critical. We made our way across into information working several years ago and cannot go back. Ten years ago we had difficulties with feed interrupts. We still have feed interrupts but the software now takes account of shortfalls.	1. Critical 2. Transition to electronic ways of working irreversible 3. Software can compensate for interruptions to service	309. New working practice
E Q4	Information is fundamental to doing business. [Also] Inconsistent, it is frequently difficult to find a unique single source of truth. There are multiple information sources which are not consistent. We (C4ISTAR and HQ) have many Campaign Plans for example. They are not co-ordinated and often at odds. [Finally] Incoherent, coupled with the inconsistency means we do not see good practice which leads to an inconsistent approach. This leads to hard work for people.	1. Fundamental 2. Inconsistent 3. Incoherent	310. Information management 311. Single source of truth 312. Security practice
F Q5	Not enough value placed on good information and this is not understood. For example, looking at encyclopaedic data, systems need this information for business processes and as data to process. Missing or low quality data leads to poor output. Not sure if others (RN) understand this concept. We create mountains of data which is useless. Again the Campaign Plan is an example.	1. Awareness of security practice 2. Quality and availability of data	313. Security awareness 314. Integrity 315. Availability
G Q6	There has been fallout from Burton and Hannigan. There are now tighter procedures for handling and carrying data. Security measures are enforced to stop data leaving secure areas.	1. Management reaction to security incidents 2. Changing secure working practice	316. Reaction to incidents 317. Changing people's security behaviour

Continued ....

ENG4

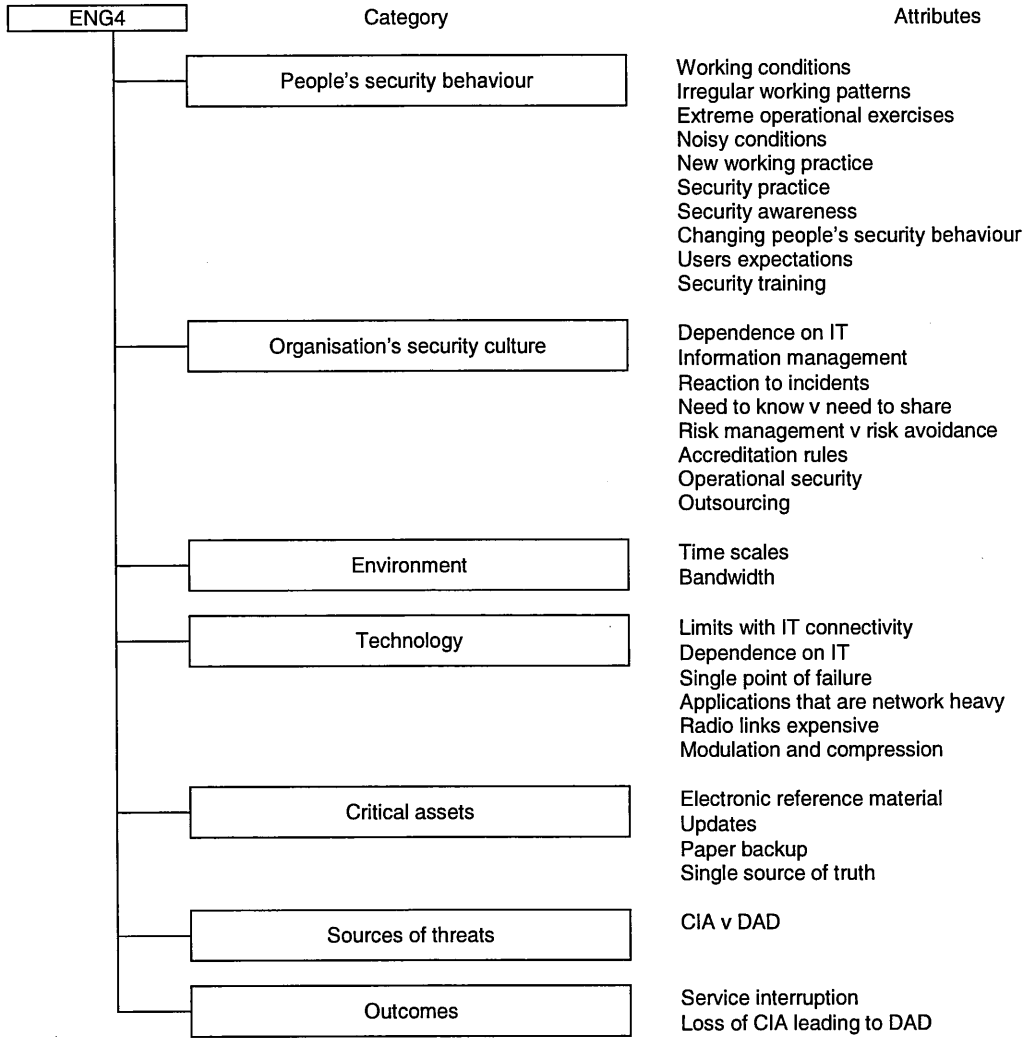
Data block and question	Interviewee's opinions of maritime environment and ICT security	Researcher's interpretation of interviewee's opinions	Research code
H Q7	It can be devastating really. In 2000 -2002 we set up CSS. Within a short time ships became dependent. If you have a server crash or lose connectivity then it takes time to get back into old ways of working. This can lead to User frustration and lost key information for making decisions and blind to background material.	1. Rapidly became dependent on IT 2. Causes frustration when not available 3. No real alternative 4. Can lead to loss of information	318. Dependence on IT 319. Users expectations 320. Single point of failure 321. Loss of integrity
I Q8	Without data, the business process would not go on. It would take longer to do things. Reverting to formal messaging would be a nightmare. We are building in firewalls and constraints, limiting file type transfers and harmful packages. But in coalition there must be a balance between security and openness.	1. Interruption to data flow would cause operational problems 2. Balance needed between need to know and need to share	322. Interruption 323. Need to know v need to share
J Q9	Predominately risk based approach to systems and day to day information they contain. It can be erratic and can slow down the speed of progress when trying to get new systems etc. However, there are good reasons for doing it. For example, the RN Command Support System (CSS) followed accreditation procedure but not when operational. Playing lip service to security measures runs the risk of completely corrupting the operation.	1. Risk management v risk avoidance 2. Former needed latter can lead to delays 3. Accreditation process followed for procurement of CSS. Now that it is operational, security is processes are not being enforced.	324. Risk management v risk avoidance 325. Accreditation rules 326. Operational security
K Q10	The CSS [Command Support System] requirement was defined as a closed system in the late 1980s then as it became operational more and more connections were needed. In the original design, nobody considered that file transfer would be needed. But now we have User error transferring file from new server system. CSS Security Operating Procedures (SyOps) would have prevented this in the old days but new design for flexibility not locked down.	1. Impact of connecting disparate systems not understood 2. The need for flexibility can be used as an excuse to override security processes	327. Accreditation 328. Operations v security
L Q10	Security training poor from both an information systems and information technology view point. I recently completed an information assurance course. Otherwise I have no formal training. I have never been an IT Security Officer (ITSO) although I have had ITSOs working for me. With only a few hours training I have to read books to catch up. I have had jobs where I should have known more but never received training. We seem to rely on expensive gurus now!	1. Security training for systems and information is poor 2. IT security officer can be a second or third job 3. Outsourcing	329. Training 330. People 331. Outsourcing
M Q11	It will largely track policy and plans for fixed architecture. This presents problems in the working environment. One of the problems is the accreditation for combat systems. We have to apply information systems accreditation to combat and legacy systems interactions.	1. Accreditation process	332. Accreditation

Continued ....

ENG4

Data block and question	Interviewee's opinions of maritime environment and ICT security	Researcher's interpretation of interviewee's opinions	Research code
Q11, Q12, Q13 and Q14	Omitted because of time constraint		
N Q15	It's not really different, in fact not so many points of penetration. We have good protection and radio encryption.	1. Points of penetration (physical boundary around the hull). 2. Radio encryption	333. Physical security 334. Radio encryption
Q16	Omitted because of time constraint		
O Q17	The speed of change is so great. The big problem is that we are the poor cousins in terms of bandwidth and most information systems take little consideration of bandwidth [e.g. synchronous v IP].	1. Rapid time scales 2. Poor bandwidth 3. Applications can be network heavy	335. Time scales 336. Bandwidth 337. Network heavy
P Q17	At home you can expect broadband and more. On-board ship there is a single input path, which is expensive, technically limited and so we are constrained.	1. Ship radio connectivity expensive and technically limited	338. Radio links expensive
Q Q17	We must concentrate on bandwidth efficiency to make (maritime) solutions useable.	1. Need to improve modulation and compression techniques	339. Modulation and compression

ENG4: Summary of initial analysis



CIS1 26th August 2009

Data block and question	Interviewee's opinions of ICT security in a maritime environment	Researcher's interpretation of interviewee's opinions	Research code
A Q1	Undoubtedly yes. The environment in terms of its hostility both the enemy and also the elements. Predominately, in my area of business, it is the limited bandwidth which presents a constraint which is not frequently remembered with ease by those within the wider communications C4 [Command, Control, Communications and Computers] community.	1. Hostile enemy 2. Hostile elements 3. Bandwidth constraint 4. Those working in land environment not always aware of limitations with ship to shore communications	340. Environment - enemy 341. Environment – elements 342. Bandwidth 343. IT limitations
B Q2	Personally? I think the breed of 'Luddites' have gone and I think, in the main, there is a universal recognition that information technology is your life blood. The linkage is to decision superiority, which is ultimately what senior officers at sea are there to do; not to be managers but to make decisions.	1. Lifeblood 2. Information for management 3. Information for decisions	344. Lifeblood 345. Information for management 346. Information for decisions
C Q2	Decisions are completely dependent on good information and therefore the realisation is that one needs to assimilate as much relevant information as possible and that therein lies the challenge of information management, to ensure that Commanding Officers brains are not be befuddled with a lot of material that is not relevant. So, I suppose the short answer is that I would be totally reliant upon IT.	1. Quality of information 2. Information management 3. Totally reliant on IT	347. Quality of information 348. Information management 349. Totally reliant on IT
D Additional question 1	How do you think this will evolve?		
	I think it will clearly grow the ability for external micro management and will drive the need for ships at sea to provide more information ashore to spread local situational awareness and to contribute to the wider picture. But the evolution that must take place is that proliferation of information will drive the requirement for smarter information management and for the need for local specialists to provide that service of information management information packing; not necessarily producing information or using information but just ensuring that it is presented in the best way possible to enable it to be rapidly assimilated.	1. Spread of IT will enable micro-management from ashore 2. Ship's will provide information to improve situational awareness 3. Smarter information management 4. The need for local specialists to advise on information continuity and format	350. Command and control 351. Local responsibility v micro management 352. Information management 353. Information experts
E Additional question 1	Obviously, one of the evolutions is the significant change that we are trying to introduce in the naval intelligence capability where we believe we do need enduring specialists who can provide that service to the Command. The Command obviously needs to be hungrier for the products that sometimes they are unaware of. I think we recognise that intelligence is just a subset of information. It is special information that comes, often, from sensitive sources and comes with analysis. It still needs effective management.	1. Specialist information exploitation 2. New intelligence capability	354. Specialist information exploitation

Continued ....

CIS1

Data block and question	Interviewee's opinions of ICT security in a maritime environment	Researcher's interpretation of interviewee's opinions	Research code
	Do you foresee any barriers to achieving this evolution?		
F Additional question 2	Yes, I think the technological barriers are falling. I think we are still significantly hampered at sea by bandwidth and the cost of it at the moment – we live in austere times. Linked to that are the technologies that are in play frequently assume continual presence and high bandwidth which is not necessarily the case for warships and submarines that dive or ships that need to maintain EMCON silence.	1. Technological barriers are playing less of a role 2. Bandwidth 3. Service costs 4. Operating conditions and circumstances dictate how and when IT can be used	355. Technological barriers 356. Bandwidth 357. Outsourcing 358. Security v operations
G Additional question 2	The major barriers, I know, are cultural and it is maintaining the risk balance between the benefits of sharing and the risks of inappropriate sharing or operational compromising of operational security.	1. Cultural 2. Maintaining balance between need to share and need to know	359. Cultural barriers 360. Need to share v need to know
H Q3	As ever it is fundamental. Historically, the sparsity or the limitations of communications technology have encouraged, or fostered, a degree of independence which has been cherished by mariners. Some would say that, unfortunately, technology has begun to erode that. But never the less I think that the senior management within the Navy, at the moment, still fosters that independence of Command thought; I think so as to ensure that there is not an over reliance on communications which have that ability to micro manage from shore.	1. Autonomy v micro-management 2. Loss of autonomy due to better connectivity 3. Must not let IT erode command and control	361. Autonomy v micro-management
I Q3	Though technically feasible and tempting, it is not 100% assured and therefore for resilience purposes it makes a lot of sense. It is predominately our main communications pipe which is the external stimulus that would otherwise make our life at sea very insular.	1. Continuous links to shore would be very expensive and not always possible 2. IT used as an impetus for improving ways of working	362. Ways of working
J Q4	I could be flippant and say chaotic! It is certainly sub-optimal. It is incoherent and aspirational. There is a huge desire to do better. I think that there is a realisation that we could do a whole lot better. So, the aspiration is there and people would like to do better.	1. Chaotic – not as good as it could be 2. Incoherent 3. Aspirational	363. Ways of working
K Q5	Yes, but, it does not often behave as if it truly recognises its importance. I would say that, particularly in this headquarters organisation and I think that you could extend it to the wider Navy in most instances, we are information management organisations. When you ask us what we do, people will talk about generating force elements at readiness.	1. Importance of information recognised	364. Information management 365. Information for operations support

Continued ....

CIS1

Data block and question	Interviewee's opinions of maritime environment and ICT security	Researcher's interpretation of interviewee's opinions	Research code
L Q5	We don't, we take information in and we generate information out which others act on. That is what actually results in those hard outputs. The vast majority of this headquarters outputs and inputs are information. So yes; we have got the previous First Sea Lord to state, in some of the documentation associated with our new information governance and structures, that information is the life blood of the Royal Navy. We cannot do anything without good information on which to base our decisions and actions.	1. Information management 2. Information governance 3. Information for decisions and actions	366. Information management 367. Information governance 368. Information for decisions and actions
M Q5	I hope the answer to 'how does the organisation protect information' is, in a structured way recognising the differences between physical security and 'cyber' security; but clearly the latter is evolving.	1. Cyber security is evolving	369. Cyber security
N Q5	In governance terms we are challenged by the fact that our key elements of information and knowledge, that we wish to protect, are increasingly held in electronic form and the current 'flavour' of our protection regime is very much centred on recent, very public, breaches of personnel data. Therefore, the pendulum has swung back towards the 'need to know' and a focus on protecting information and not sharing, rather than deriving the benefits of sharing. There are a range of publications, such as JSP 440, and others which we use for guidance on a daily basis.	1. Information and knowledge base held in electronic form 2. Need to know taking precedence over need to share as a response to security incidents	370. Need to protect electronic environment 371. Management reaction to security incidents
O Additional question 3	How effective are these publications?		
	They are not as effective as they could be because they largely don't address the cultural aspect which is where we need to work. I suppose in terms of approach we are trying to use a risk management approach which should mean that those involved in aspects such as accreditation are not actually empowered to say no. All they can do is arm the decider with the information as to the risk.	1. Security rules and guidelines do not address the cultural aspects 2. Accreditors need authority to act	372. Security culture 373. Accreditation
P Additional question 3	I think that one of the key issues at the moment, in a risk based approach, is trying to identify who the risk owner is and increasingly as our networks proliferate and become entwined, those who might have thought they were empowered to take an information risk may be jeopardising an entire network and therefore they are not. The key challenge is to work out who is empowered to accept risk.	1. Need to identify the owner of the security risk in situations where networks become interconnected	374. Risker owner

Continued ....

CIS1

Data block and question	Interviewee's opinions of maritime environment and ICT security	Researcher's interpretation of interviewee's opinions	Research code
Q Additional question 3	A strand of that answer 'how do we do it' is also, not as well as we could or should and that is based, primarily, on our inability to know what it is we have got to protect. The issue, again on the personnel data front, is compiling an information asset register, and this information asset terminology ostensively applies to all information assets; but we still really cannot get a crisp definition of what an information asset is.	1. Do not understand the sale of the problem 2. What is an information asset?	375. Scale of the problem 376. Information as asset
R Additional question 3	By inference, if it isn't an information asset then it is an information liability you should probably get rid of. The thinking is, predominately, that an information asset is a key element of information that underpins any process within Defence and therefore it is the process owner who is in a position to decide what constitutes an information asset and how it is to be controlled. That thought process is leading onto the next question.	1. If information is not an asset then it is a liability 2. Information owner	377. Information as asset 378. Information owner
J Q6	Information Assurance has changed rapidly in the last few months as a result of responding to the public data losses and the Information Commissioner effectively putting the MODUK on quarterly report. The change has primarily been to a reactive stance closing off weaknesses that have been identified by Sir Edmund Burton and the Data Handling Review. We have yet to move to the more proactive stance.	1. HMG undertaking close scrutiny of MODUK because of data losses 2. Move from reactive to proactive security stance	379. Management response to incidents 380. Reactive v proactive security
K Q6	Key amongst the changes is a new lexicon, including new titles, provided to us by the Cabinet Office and a new governance structure that we have had to stand up within the Naval Service. This has switched the focus of senior level information risk ownership and management from ACNS who was the titular Chief Information Officer, it was largely titular, down to this headquarters and to anointing DCINC as the Command Information Officer and Senior Information Risk Owner. Primarily because, as Chief of Staff for the headquarters, he is best placed to pull the levers that would get things done.	1. New job titles 2. New security responsibilities	381. Management response to incidents
L Q6	There have been a lot of changes and a number of them have been less than coherent. Perhaps some of them are somewhat reactive with Cabinet Office directives being passed on from the Centre to TLBs without necessarily any sort of value being added in terms of the applicability or implement-ability of some of these directives.	1. Change has not been for the better 2. Cannot apply all the new security requirements in all situations	382. Change not thought through

Continued ....

CIS1

Data block and question	Interviewee's opinions of maritime environment and ICT security	Researcher's interpretation of interviewee's opinions	Research code
M Additional question 4	Is this a barrier to achieving future success if we are struggling with this at this stage, when we get Network Enabled Capability is it going to get worse?		
	No I do not think so. It has got to get better it is so important. The focus for that improvement, which we have now been given, is the Information Assurance Maturity Model which is giving us a bench mark against which to compare ourselves and hopefully a hit list on the road to improvement.	1. Changes must not be allowed to become barriers 2. Working towards improvement with IAMM as benchmarking toll	383. Security behaviour
N Additional question 4	So we have assessed ourselves against that pretty subjectively at the first pass and identified that we are at a low level, not at the bottom but low, and so an ambitious target has been set to get from level one to level three by 2012. That will be critically dependant, as ever, on resource; but key amongst that will be the cultural change programme which is where many of the failings against that maturity model are.	1. RN starting from low level but intend to improve rapidly 2. Cultural change programme 3. Improving security is resource dependant	384. Security behaviour 385. Cultural change 386. Resources
O Additional question 5	It has been suggested by other interviewees' that the IAMM is an overreaction?		
	I think to a certain extent we needed those public losses, in a way, as a wakeup call and a catalyst for the change which otherwise might have been so slow in coming that it would not have achieved the rapid results that hopefully we will now get and have always needed.	1. Incidents have forced change to take place	387. Security behaviour 388. Cultural change
P Additional question 5	Key amongst this is role out of DII (F) as a ubiquitous infrastructure in Defence and our relative unpreparedness for that and the ability to exploit the benefits it should bring. In most instances, particularly in the circles I move in, we have been overly focused, necessarily so, on the technical aspects and have not been able to devote energy that we probably should have done to exploiting the benefits.	1. Ubiquitous infrastructure 2. Get the technology out there, then worry about how to use it was the wrong approach	389. Exploit the befits
Q Additional question 5	Our I-hub team down below, who were configured to take forward information exploitation initiatives across the TLB, have become almost exclusively involved in account management not just for the DII role out but just with managing the day to day churn that results from normal appointing and organisational change which is endemic.	1. Information management team not being used to their full potential	390. Security behaviour

Continued ....

CIS1

Data block and question	Interviewee's opinions of maritime environment and ICT security	Researcher's interpretation of interviewee's opinions	Research code
R Q7	Well, in part we in the Naval Service prepare for and train to cope with the loss of external connectivity. But within Units we are just so totally reliant on it for situational awareness and management of the platform	1. Practice loss of connectivity 2. Internal dependence absolute and loss of IT not practiced	391. Connectivity 392. Contingency
S Q7	Examples being the conficker virus and the realisation that, though ostensively it was an operational support capability that was denied us, the boundary between operations and operations support is increasingly fuzzy and the realisation of Health and Safety implications. RFAs have their safety manuals resident on those systems. So, if they could not access them then, in theory, they could not go to sea. We are dead in the water without the system.	1. Operations v operations support 2. Total dependence on the IT system	393. Boundaries of responsibility 394. Dependence on IT
T Q8	Yes, increasingly our drive towards a ubiquitous network does make us a more attractive target and the potential for more significant impact if an adversary is successful. However, the counter argument is that it allows us to introduce more effective protection and awareness of our networks health and the attacks to it.	1. Ubiquitous network increases vulnerability 2. Increased vulnerability improves effort towards new understanding of the problems	395. Ubiquitous networks 396. Can have positive effect
U Q9	That is certainly a growth area. We have within the Naval Service a WARP, the Warning and Reporting Point which is within the bailiwick of PSyA; though increasingly the people there don't have the level of skill to understand the messages they are passing on and very often they are shouting from the roof top not necessarily knowing who they are expecting to acknowledge it. That is why my team will become more involved.	1. The need for incident response capability 2. New skills needed	397. The need for incident response capability 398. New cyber security skills needed
V Additional question 6	Is there scope for a Computer Emergency Response Team on-board? Is it worth having a small team on-board?		
	In effect you do. The Weapon Engineering team hopefully have that expertise and are configured for battle damage repair. I think you are right that the cyber battle is continuous and spontaneous and therefore yes that battle damage repair team will have to acquire more of the skill sets which in part they have already got through the system engineering skills and their system management skills. It will need augmentation from shore. The first line of defence is system knowledge and maintaining the system at the correct patching state.	1. New cyber security skills need 2. Shore side support needed 3. Need to have intimate understanding of how IT works as a whole	399. New cyber security skills needed 400. Shore side support needed 401. Systems thinking

Continued ....

CIS1

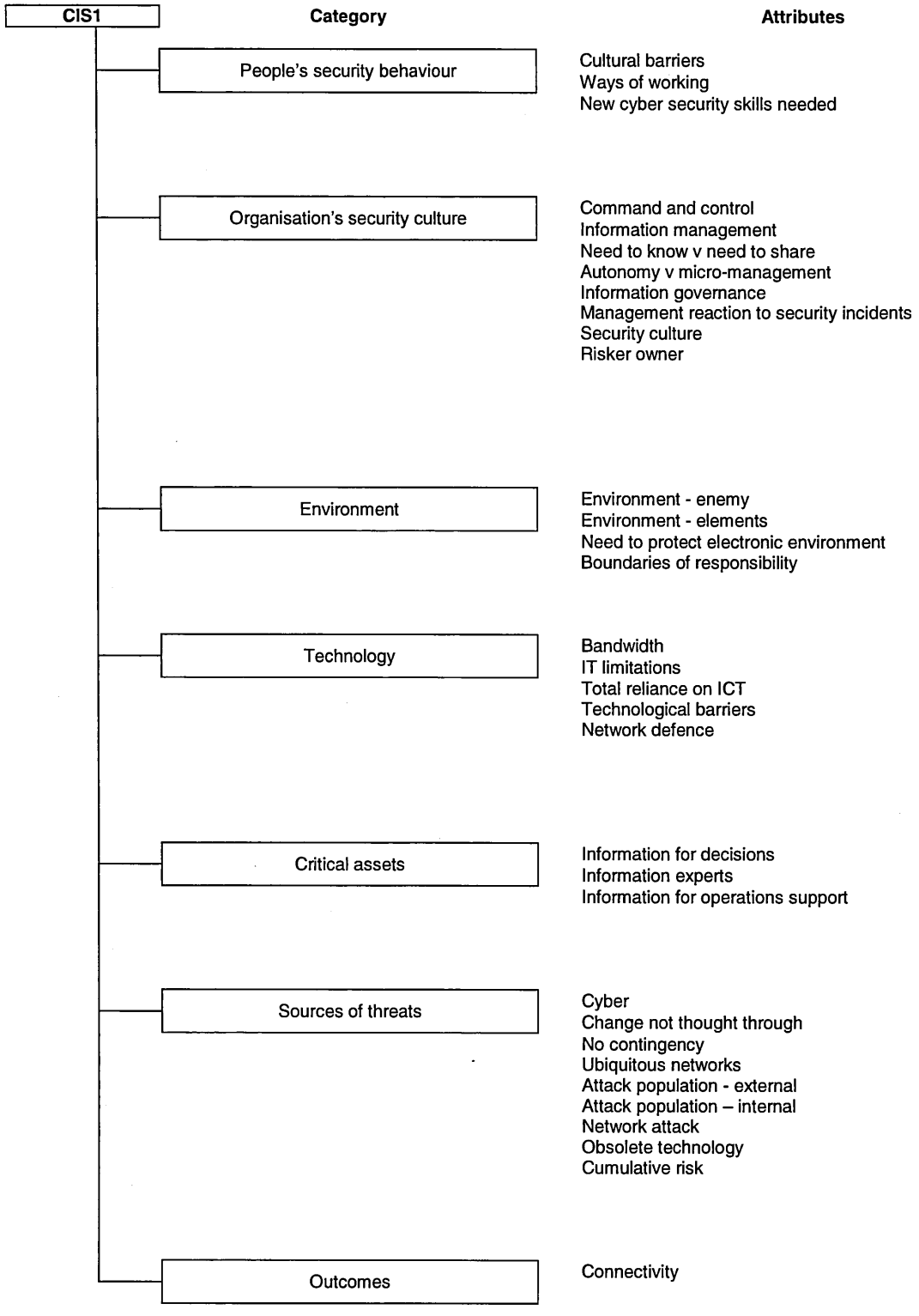
Data block and question	Interviewee's opinions of maritime environment and ICT security	Researcher's interpretation of interviewee's opinions	Research code
W Q10	It is primarily cultural. You should be aware that Permanent Undersecretary of State has directed that everybody in Defence, along with all other Government Departments, is to receive some information security awareness training. The major focus is personnel data but not exclusively so.	1. Need to change security culture from top to bottom 2. Need security training and awareness from top to bottom	402. Security culture 403. Security training 404. Security awareness
X Additional question 7	Are you aware of any other issues that lead to security incidents?		
	There is the ill-disposed external attack; but I think by far the majority of security incidents are own goals. Now we rather more overtly talk about the fact that we not only do computer network defence but we have a latent computer network attack capability within Defence working on the premise that if we understand how we might attack other peoples systems we better understand how they might attack ours.	1. External attacks 2. Mostly internal problem 3. Network defence 4. Network attack	405. Attack population - external 406. Attack population – internal 407. Network defence 408. Network attack
Y Q11	I think it will, in the near term, continue to be seen as an N6 [CIS Division] function and that the focus will be on technology and accreditation. My fond hope is that increasingly it will become an N3 N5 function. I see your question relates to IT risk, but I would say it is information risk where there is a better understanding of process and process ownership and therefore who is empowered to manage risk, decide 'what are your key assets to be protected' and developing a proper risk management approach rather than an ad hoc one.	1. Short term focus will continue to be technology and accreditation 2. Longer term, personal awareness and intelligence will become imbedded in the security mix 3. Information risk involves process and process ownership so that the right people can make the right decisions based on accurate information	409. Accreditation 410. Imbedded security awareness 411. Information risk management
Z Q12	Yes that is true. To a certain extent our weakness or exposure to the conficker virus was in part that sort of decision. Those systems that we had hoped would be replaced by new, where still in existence and the cost of testing and applying patches was a factor in the delay in their implementation thereby leaving us exposed to a weakness.	1. The risk involved with running on obsolete systems causing problems	412. Obsolete technology 413. Cumulative risk
AA Q12	I think the challenge, in the context of cumulative risk, is ensuring that in our approach to the governance of information risk that the right person is identified to track and assess that cumulative risk. There may be a number of people that are aware of elements of risk but in the new information risk management approach, and it is one of my new roles, potentially, as the Senior Information Risk Owners Information Risk Manager to try and expose to him what that cumulative risk might be and that it is identified in the first place.	1. New role in tracking cumulative risk.	414. Cumulative risk

Continued ....

CIS1

Data block and question	Interviewee's opinions of maritime environment and ICT security	Researcher's interpretation of interviewee's opinions	Research code
BB Q13	I think that that is a splendid example. In my previous existence in the DCSA [Defence Communications Services Agency], when I was challenged by General Rapper to get under the skin of industry, the cry from a number of people was 'well it's all very well talking to industry they can cut corners because people don't die if they get it wrong'.	1. Industry cut corners to make profit	415. Security behaviour
CC Q13	But banks would probably beg to differ. In the business health sense they would die if they screwed up big time and therefore they are incentivised almost to the same extent as we are for safety critical software. So, yes I believe we should be looking closely at that.	1. Lessons from other sectors are important	416. Lessons cross sectors
DD Q14	Applying the risk management approach is the best methodology. To say that, in theory, nothing is off limits and that appropriately advised and once the risks had been properly assessed then there is the scope to adopt.	1. Risk management depends upon proper assessment and guidelines	417. Risk management
EE Q15	By inference we might think that we are potentially at less threat because of the tenuous nature of our connectivity and our lack of continual presence makes us less attractive to external attack. I think the internal vulnerabilities are just as acute and the impact is potentially more acutely felt through the lack of expertise on-board and the lack of the ability to rapidly ship in that expertise. Once again, the bandwidth constraints to remotely apply patches and reach back to the hub. Physical security is much improved - you have a tin box around you to protect and deter.	1. Non-permanent connectivity reduces vulnerability 2. Internal vulnerabilities include lack of IT expertise 3. Bandwidth 4. On-board physical security well covered	418. Connectivity 419. Lack of IT security expertise 420. Bandwidth 421. Physical security

CIS1: Summary of initial analysis



CIS2 21st July 2009

Data block and question	Interviewee's opinions of maritime environment and ICT security	Researcher's interpretation of interviewee's opinions	Research code
Q1 and Q2	Omitted because CIS2 has no sea going experience		
A Q3	Same as an HQ environment. The purpose is different – to run a ship, but the way should be very similar. When personnel move ashore the principles should be the same. There is a massive role for information from sensors to intelligence to administration to keep the ship running. Information overload very important to avoid in the afloat environment. It happens in HQs as well. It's a nuisance in HQ, but afloat could be dangerous.	1. Transferable skills 2. What could be a nuisance ashore could be a serious problem afloat	422. Transferable skills 423. Barrier depends upon prevailing conditions and circumstances
B Q3	We need to reduce overloading. There is no technology in place. Much is cultural and behavioural like guide lines and protocols. My experience is that no one adheres to them. For example, I receive information copies of e-mail which takes time to wade through. It's about push versus pull. The technology is emerging to enable pull. Although the technology will not be used properly until the critical mass working that way. Such as posting information etc. The afloat solutions coming soon.	1. Information overload 2. Culture and behaviour 3. Push v pull	424. Information overload 425. Change security culture 426. Change security behaviour 427. Push v pull
C Q4	Inconsistent: People have inconsistent levels of experience. Team Site use is inconsistent, people still use attachment versus instead of links. We are not as bad as other Divisions. Improving, slowly, our use of information. This is a general problem – do not appreciate collaborative working versus dissemination or publish to wider audience. One more – records management is a problem area for everyone. This partly due to poor tooling and partly poor culture.	1. Inconsistent experience 2. Inconsistent behaviour 3. Improving slowly 4. Records management poor due to technology and culture	428. Lack of experience 429. Change behaviour 430. Records management
D Q5	Very much so, led by ACOS. Absolutely as you would expect for C4ISTAR.	1. Information is an important asset	431. Information as asset
D Q6	If we go back one year then massive. Personal data encryption rules using approved products; removal of hard discs and memory sticks off site; and cultural changes have led to a much better understanding of the need to protect Information Assurance assets. For my Section this has led to more procurement action.	1. Changing security culture	432. Changing security culture 433. Changing security behaviour

Continued ....

CIS2

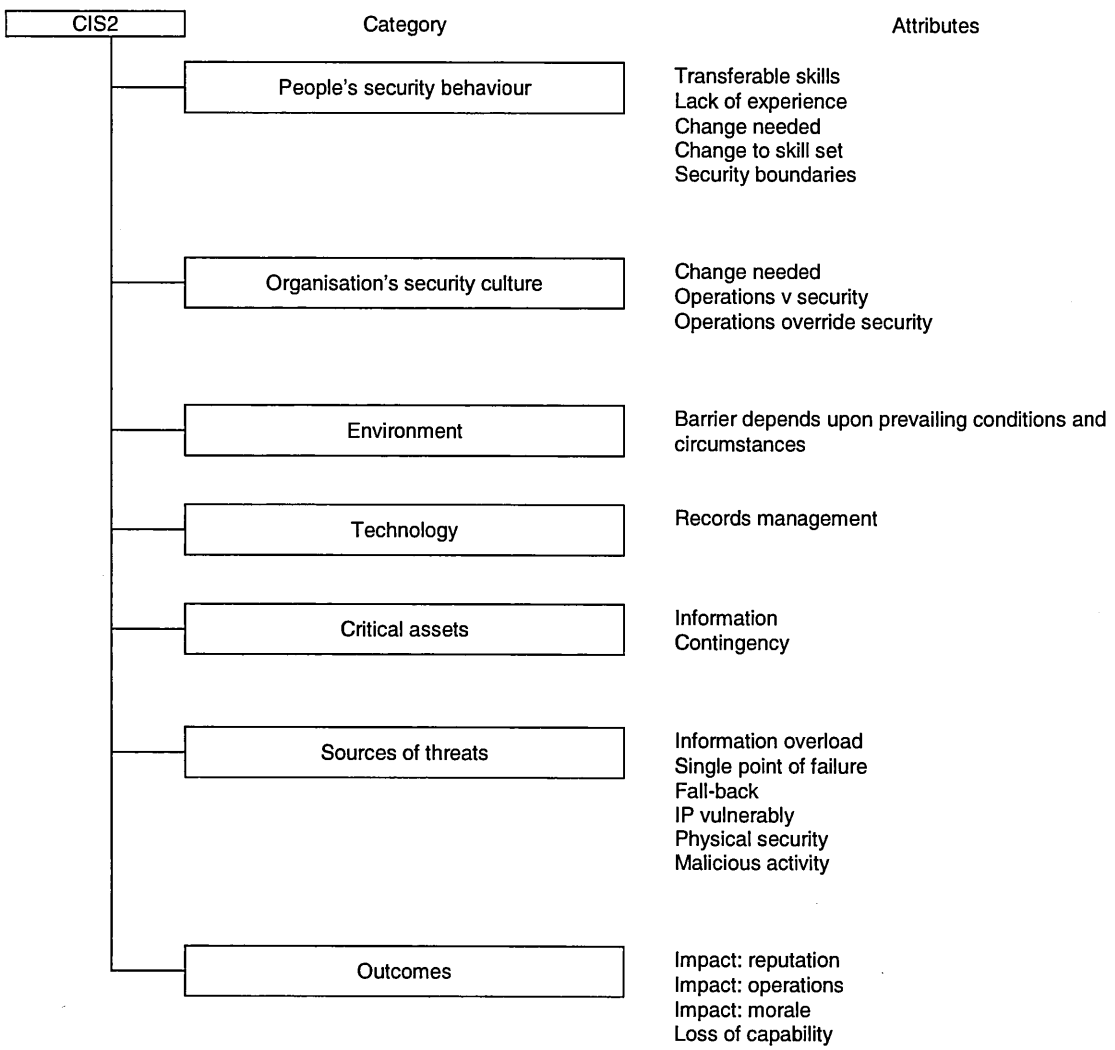
Data block and question	Interviewee's opinions of maritime environment and ICT security	Researcher's interpretation of interviewee's opinions	Research code
	Certain interviewees have suggested that HMG have overreacted. Would you like to comment?		
E Additional question	Yes, I think initially there was a knee jerk. But common sense coming through. Deadlines for optical media have been extended. The difference between personal and protective marking has more sensible discrimination. Whether we can meet new timelines is debateable. Risk balance cases are being accepted if shown to be working towards full compliance. Burton and Hanigan reports take the utopian position. It is up to the Department (MODUK) to take sensible path. Especially after the impact of the losses. Everyone more sensitive – For example, if I take my laptop (off base) I carry it with me rather than leave in the car.	1. Sensitivity to security issues is changing	434. Security behaviour
	Will the sensitivity stand the test of time?		
F Additional question	It is a risk unless constantly reinforced. Must be embedded in operations and daily business then it will be ok. We are not at that point. We need constant reinforcement. Information Assurance must reset target or fade. Should be on same footing as diversity etc. Treat like that or it will fade again.	1. Could lose momentum if not constantly reinforced with security awareness campaign	435. Security culture 436. Security behaviour
G Q7	First thing is the reputational impact on MODUK and certainly on the (Royal) Navy. Reputation is more than real impact. In extreme circumstances it could have an impact on operations, but this is rare. If you know then you can do something. There is a morale issue – if one of my team lost something now I would be very angry. It would do C4ISTAR damage. We set best use practice and set an example to others.	1. Impact on reputation when things go wrong 2. Impact on operations 3. Impact on morale	437. Impact: reputation 438. Impact: operations 439. Impact: morale
H Q7	A virus could lead to the loss of capability. Conficker, for example, led to the disconnection, of certain Units, from the RLI leading to a temporary loss of capability. This example with NAVYSTAR became inconvenient. We have fall-back at the moment. That's the worry about putting all across DII.	1. Impact: loss of capability 2. Loss of contingency once all on one network	440. Loss of capability 441. Single point of failure 442. Contingency
I Q7	There is an interesting parallel with banks etc. What happens when the Internet is not available? I run my affairs on the Internet. What happens if it all falls over? Do they have fall-back?	1. Fall-back procedures	443. Fall-back 444. Contingency

Continued ....

CIS2

Data block and question	Interviewee's opinions of maritime environment and ICT security	Researcher's interpretation of interviewee's opinions	Research code
H Q8	I have never heard of a virus on military messaging. We have more vulnerability to hacking into IP systems. The more reliance on technology then the experienced hackers will look to exploit in terms of malware and executable code.	1. X25 systems are inherently safe because of their architecture 2. Vulnerability lies with IP networks	445. Legacy systems 446. IP vulnerabilities
I Q9	The other issues – more sophisticated and on-board support requires extra skills and on-board support. Extra skills required by MSP for example the NAVYNET maintainer skills will need uplifting. Perhaps not extra more like different skills. On the other hand system skills and redundancy minimise single point of failure. The one positive thing is you have a self-contained environment (at sea). You can disconnect and still run. Core node loss shore side means lost data.	1. Change to on-board skills required 2. New skills required 3. Secure box at sea	447. Change to skill set 448. Physical security
J Q10	It has been, no doubt, with people carrying laptops in cars and airports – not carrying dongle and laptop separately. In my opinion it is probably the major cause of security incidents. The other cause is people under pressure to deliver output. For example sending data over the Internet and going astray. Senior officer needs to get this information and the Internet is the only way to do so. Achieving output is more important than security.	1. Laptops outside of the physical security perimeter 2. Pressure of work leads to shortcuts 3. Operations takes precedence over security	449. Security boundaries 450. Changing people's security behaviour 451. Operations v security
K Q11	Only issue is the Commanding Officer is more empowered to take risk than in an HQ. Operation imperative lead to more risk than sat in HQ.	1. Operations override security	452. Operations override security
Q12, Q13 and Q14	Omitted because of time constraint		
L Q15	I suppose that you don't have permanent network connection which could reduce the vulnerability.	1. Not always connected so not always vulnerable	453. Malicious activity
M Q16	Network Enabled Capability probability brings that additional vulnerability.	1. Network working implies potential for vulnerability	454. Malicious activity
N Q17	Generally, the more IP connectivity you have that potential to exploit maliciously.	1. More connectivity implies more attack routes	455. Malicious activity

CIS2: Summary of initial analysis



CIS3 7th July 2009

Data block and question	Interviewee's opinions of ICT security in a maritime environment	Researcher's interpretation of interviewee's opinions	Research code
A Q1	Of course it does. There are specific instances. We are more secure in some senses. There are constraints due to bandwidth. This tends to lead to technical issues such as virus updates, patch information and ensuring access to latest advice and policy.	1. Secure from physical sense 2. Less prone to threats when not connected 3. Bandwidth constraints 4. Downloading software can be a problem	456. Physical security 457. IT threats 458. Bandwidth
B Q1	Physical no major changes more about information management and information issues.	1. Physical issues remain as they have been 2. Emphasis on information management and security	459. Physical security 460. Information management 461. Information security
C Q2	Increasingly, from an RN perspective, people are seeking to have new integrated support solutions with reach back. No longer want to wait to get into harbour. 365/24 coverage is expected but not always available – which brings tensions. Information management not fully thought through at sea. We do not procure for the C4 architecture to which we deliver which constrains our ability to deliver NEC.	1. Easier to seek virtual professional help from ashore 2. Expectations of IT not being met by procurement	462. Reduction in skills 463. Increased dependence 464. IT expectations
D Q3	Comes back to expectation of constantly being in touch. We expect e-mail as a minimum to keep in contact with our support agencies and we get lost in information management issues.	1. Information management issues	465. Information management
E Q3	For example, as a Charge Engineer at sea I would send signals (OPDEF) between support authority and command chain. But now, a Gun Maintainer may already have made contact and the Charge Engineer is out of the decision chain and actions taken on equipment responsible for but not know – we have not thought through information management. The Commanding Officer used to authorise signals, this is no longer the case. We recognise the problem. CO's Orders need to include orders that no actions taken until CO and Command informed.	1. Chain of command can be circumvented	466. Command and control
F Q3	It is a cultural shift from hierarchy for information to flat structures and authority to act.	1. Hierarchy v flat management structures	467. Hierarchy v flat management structures
G Q4	1. Trying hard but need to embed ways of working within culture 2. Revise our views on information – present in topical format not hierarchy. We are getting there. It may be the technology. With MOS we will be able to cut, dice and store more efficiently. You must conform now and wait for MOS. 3. Not intuitive – we need to be driven by metadata viewed in human format but in one system and one source of truth.	1. Trying hard but not yet there 2. Trying to change information culture 3. Trying to change behaviour	468. Changing culture 469. Changing people's behaviour

Continued ....

CIS3

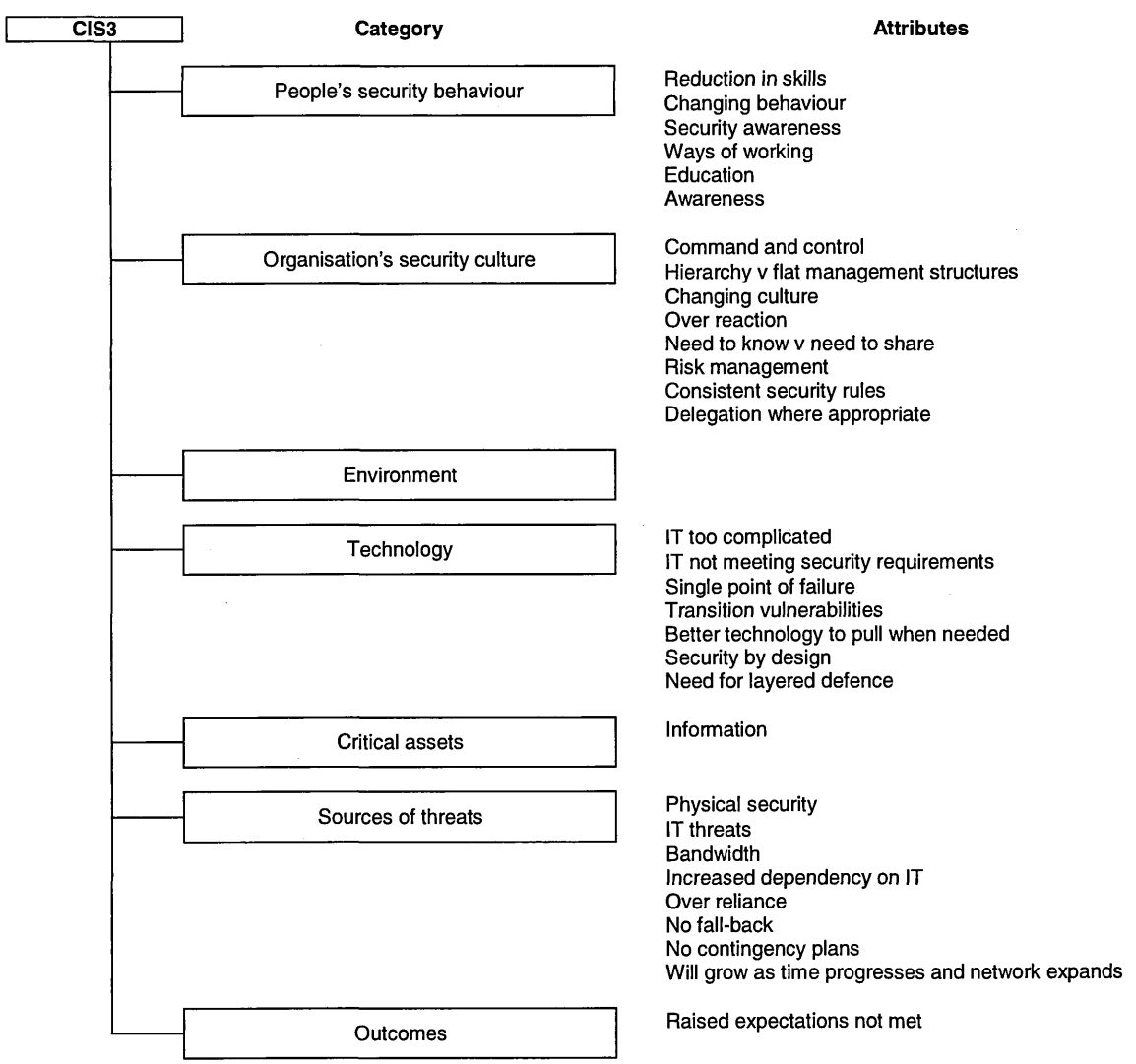
Data block and question	Interviewee's opinions of ICT security in a maritime environment	Researcher's interpretation of interviewee's opinions	Research code
H Q5	It does; we make the platitudes. However we do not we do not the resources into information management. We do not understand the ways of working. Lack the training at the basic level such as Team Sites, attachments verses links and references in documents. If you are serious SIO needs to be imbedded in business and ability to change needs to be driving from upon high. CIO (organisation) beginning to realise this. Without policies at 2 Star and higher then there will be no change. However, still resource limited.	1. Lack of understanding of information management 2. Lack of security awareness 3. Trying to change ways of working 4. Senior management needs to understand security issues	470. Information management 471. Security awareness 472. Ways of working 473. Senior management
I Q6	Two pressures in IA: Embarrassment of losses led to a review on handling procedures concentrating on the Data Protection Act. General review almost draconian taking us back to need to know, don't share and compartmentalised. Contrasting with operations and NEC pushing from the other end based on need to share. Two ends pulling in opposite directions. We are working on how to achieve both. Effective assured delivery is what we want. Timely information is needed if you are entitled to see it.	1. Outcome – embarrassment 2. Over reaction 3. Retuning to need to know 4. Conflicts with need to share	474. Embarrassment 475. Over reaction 476. Need to know v need to share
J Q7	From a general perspective – over reliance on IT to conduct some compulsory tasks with no fall-back – lack of disaster recovery.	1. Over reliance 2. No fall-back 3. No contingency plans	477. Over reliance 478. No fall-back 479. No contingency plans
K Q8	We [RN] are going to a bigger network - DII driving all eggs in one basket and afloat risk to high grade messaging. Traditional threat from current state, to new networks and the threat to support operations during transition of systems.	1. Ubiquitous network 2. Loss of command and control 3. Vulnerability during transition to network working	480. Single point of failure 481. Command and control 482. Transition vulnerabilities
L Q9	Poor understanding due to over complication and contradictory. For example, Removable media must be encrypted but technology not available.	1. Too complicated and often contradictory 2. Technology not available to meet security requirements	483. IT too complicated 484. IT not meeting security requirements
M Q10	Constant education and reminders but faced with a difficult problem. Pressure from command line and line management to achieve and output leads to 'sneaker net' use. We have to understand the risk to overcome limitations.	1. Security education and awareness pushed. Even so, shortcuts taken 2. Risk involved not understood	485. Education 486. Awareness 487. Risk management
N Q11	We need to be cognisant with business rules being applied by the organisation but hope that there would be a level of delegations: understand; greater autonomy to a certain level; and seen to get waivers. One would hope the technology would minimise the need to move data from system to system.	1. Need consistent security rules across the organisation 2. But, need delegated authority in certain circumstances 3. Network technology will help keep data in once place, one source of truth and 'pull' what you need	488. Consistent security rules 489. Delegation where appropriate 490. Better technology to pull when needed

Continued ....

CIS3

Data block and question	Interviewee's opinions of ICT security in a maritime environment	Researcher's interpretation of interviewee's opinions	Research code
Q12	Omitted because CIS3 unsighted on the issue		
O Q13	At the moment we design systems then apply security. There needs to be a step change in information systems design. With metadata it should be possible to apply security tags to information.	1. Security by design	491. Security by design
P Q14	System high approach but then have cultural approach – need to share versus system approach unless you have taken a conscious decision to use.	1. All data in one (virtual) place. Then give access to those that need to see the relevant parts	492. Security by design
Q Q15	Can apply to maritime and deployed issues such as bandwidth.	1. Threats and vulnerabilities similar afloat and ashore	493. Threats 494. Vulnerabilities
R Q16	More and more to wider threats as we grow the size of the network. The techniques are out there – we need to ensure technology for layered defence.	1. Will grow as time progresses and network expands 2. Need for layered defence	495. Will grow as time progresses and network expands 496. Need for layered defence
Q17	Omitted because of time constraint		

CIS3: Summary of initial analysis



CON1 25th June 2009

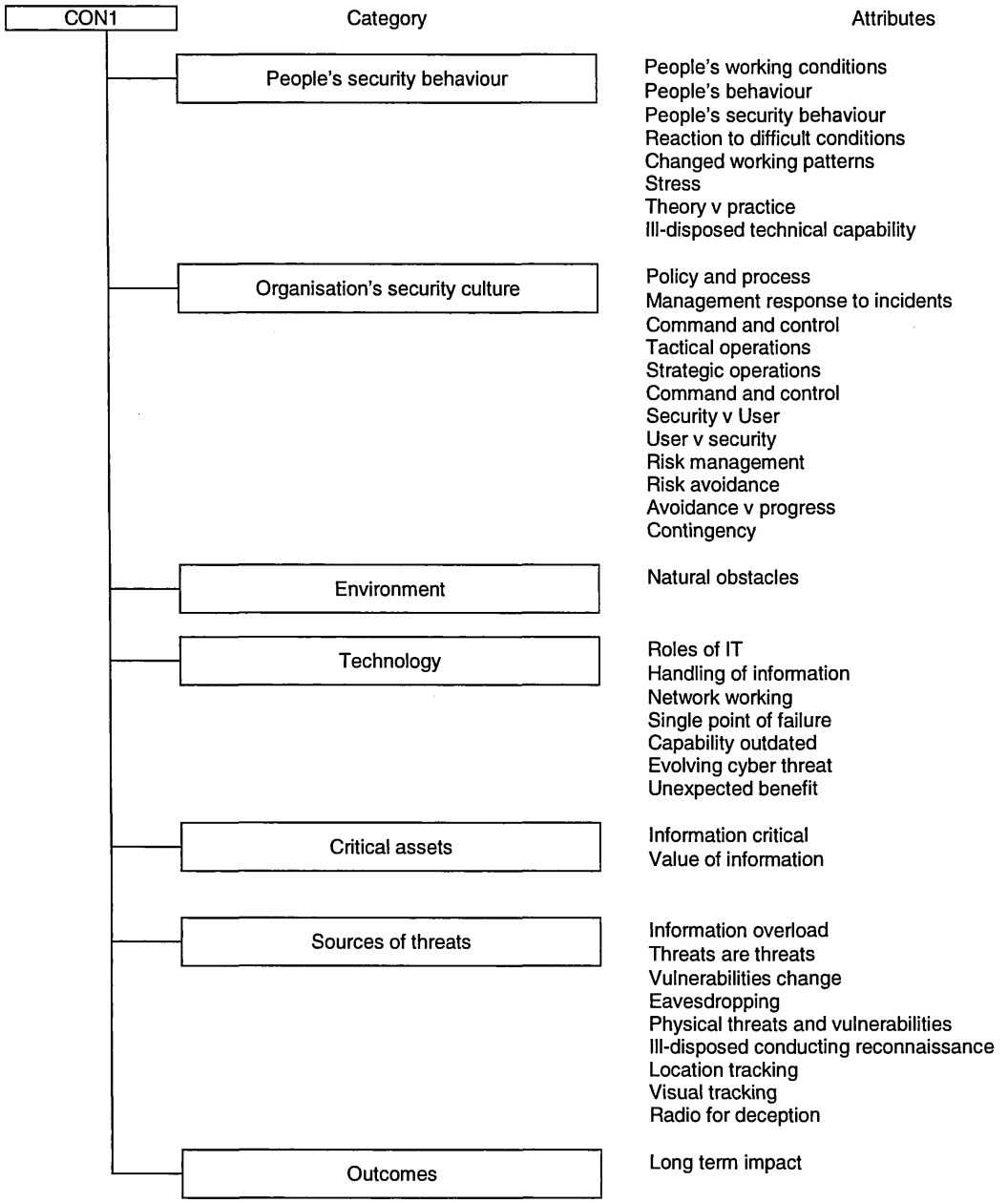
Data block and question	Interviewee's opinions of ICT security in a maritime environment	Researcher's interpretation of interviewee's opinions	Research code
A Q1	It's a relatively small community. Focus almost holey work focused with no recreation or other outlets. The physical environment can be challenging, the weather, sea states and cold.	1. Close knit community 2. Work centric 3. Weather can be counter productive	497. People's working conditions 498. People's behaviour 499. Natural obstacles
B Q2	There are the long working hours with disrupted sleep patterns. The confined space and closed community can lead to tension. Personal issues can exist and you have to be flexible.	1. Working conditions 2. Psychological problems 3. Inter-personal problems	500. People's behaviour 501. Reaction to difficult conditions
C Q3	All the roles that IT plays in any business setting.	1. Roles of IT the same afloat and ashore	502. Roles of IT
D Q3	IT used to be disjointed. It was not long ago that when you sailed you disconnected from the organisation and infrastructure. In a period of 20 to 25 years that has radically changed. The rate of change has increased and network enabled ships leads to longer detached working. This all feeds the stress already caused by the environment. I think it must be horrendous to be at sea and being fed by the e-mail machine – information requests, enquires and demands.	1. Move from isolated working to virtual real-time connections 2. Leads to increased stress from incessant push of information and requests for information	503. Changed working patterns 504. Stress 505. Information overload
E Q4	The life blood for any organisation. Information, that's how all organisations work. Even a simple example of a corner shop. They need to know their customer requirements, shopping habits and suppliers.	1. Life blood.	506. Information critical
F Q5	It thinks it does. But it does not truly understand the value of the information it has or treat handling and processing with the kind of value it ought to.	1. Value of information not understood 2. Handling of information could be better	507. Value of information 508. Handling of information
G Q6	This has had impact both good and bad. Whilst the loss is bad and clearly lax policy and procedure allowed loss. Reaction to the loss is having a disproportionate effect which is hampering the use of information to best effect. It may be solving the problem we have but massively overcompensating which has caused more problems which may in time prove to be more adverse than the loss of personal data in the first place.	1. Lax security policy and process 2. Disproportionate response 3. Caused more problems 4. Long term impact not known	509. Policy and process 510. Management response to incidents 511. Long term impact
H Q7	To our organisation you would immediately stop current dynamic command and control capability. This would impact on any form of decision making. You would isolate forward deployed decision makers from their sources. Wider scale activity direction would be lost and loss of interaction. They would use different words in a commercial organisation but same effect.	1. Loss of command and control 2. Decision making lacks information 3. Isolate widely dispersed units 4. Strategic decisions compromised	512. Command and control 513. Tactical operations 514. Strategic operations

Continued ....

CON1

Data block and question	Interviewee's opinions of maritime environment and ICT security	Researcher's interpretation of interviewee's opinions	Research code
I Q8	Probably not truly new; much more of what we have now. Maybe the threats are there; where they pop up will change. Scale and scope will be the daunting factor. I question how much theory should make it to the practical environment. There is an issue of balance.	1. Threats are threats 2. Vulnerabilities change 3. Scale of the problem will increase with network working 4. Not keen on theory – prefers practical solutions 5. Balance between theory and practice	515. Threats are threats 516. Vulnerabilities change 517. Network working 518. Theory v practice
J Q9	One has to try to avoid single points of failure within the infrastructure. You have to make IT security that is either transparent to the User Community or extremely simple for User Community to interact.	1. Single point of failure 2. Security built or has to be User friendly	519. Single point of failure 520. Security v User 521. User v security
K Q10	Education of people is probably one of the biggest causes of failure; this is not a new challenge or issue.	1. Still not getting security education right	522. People's security behaviour
L Q10	Don't make it to complicated or boring. The current approach to IT security is not intuitive – not yet simple enough to make training etc. simple.	1. Security and so associate training too complex which equates to boring for Users	523. People's security behaviour 524. Security v User
M Q11	We must evolve a method of risk management not the current method of risk aversion – the root cause of overreaction to loss of data. We must manage, understand and deal with. If not, there will be no evolution. If driven by profit motive, organisations will understand and try to do risk management. Could become completely paralysed in a military sense constrained.	1. Risk management rather than risk avoidance 2. Senior management need to avoid risk 3. Risk avoidance equates to no progress 4. Will fall behind in technology terms and so be unable to fight cyber war	525. Risk management 526. Risk avoidance 527. Avoidance v progress 528. Capability outdated
Q12, Q13 and Q14	Omitted because of time constraint		
N Q15	Might be so, ITSy risk should be part of the overall delivering mission. There probably are. Because of physical displacement of platform to land. Therefore, point of linkage becomes point of failure, and because maritime platform alternatives and diversity are limited – not as many options.	1. Risk management should be built into operations 2. Single point of failure 3. Limited alternative routing	529. Risk management 530. Single point of failure 531. Contingency
O Q16	Will change in time. The very complexity of technology itself may limit the ability to interfere.	1. Evolving with time 2. Complexity could work in our favour. If we cannot find it they cannot find it	532. Evolving cyber threat 533. Unexpected benefit
P Q16	The wrong doer has to become more technically competent. Listening to digital signals needs a sophisticated level of technology to intercept. On the other hand they could take a physical route to disrupt, blow-up cut wires etc. More sophisticated infrastructure may be able to re-route as a result, but they still may find a single point of failure.	1. Cyber criminals require technical capability 2. Electronic eavesdropping 3. May chose a physical attack in preference to complicated technical attack 4. Technical reconnoitre	534. Ill-disposed technical capability 535. Eavesdropping 536. Physical threats and vulnerabilities 537. Ill-disposed conducting reconnaissance
Q Q17	People talk about mobile phone tracking at sea. You do not want to make it obvious when away from land, but when in sight of land or in harbour it's very difficult to hide a ship. The German commerce raiders used deceptive communications and disguises.	1. Location tracking 2. Visual tracking 3. Radio for deception	538. Location tracking 539. Visual tracking 540. Radio for deception

CON1: Summary of initial analysis

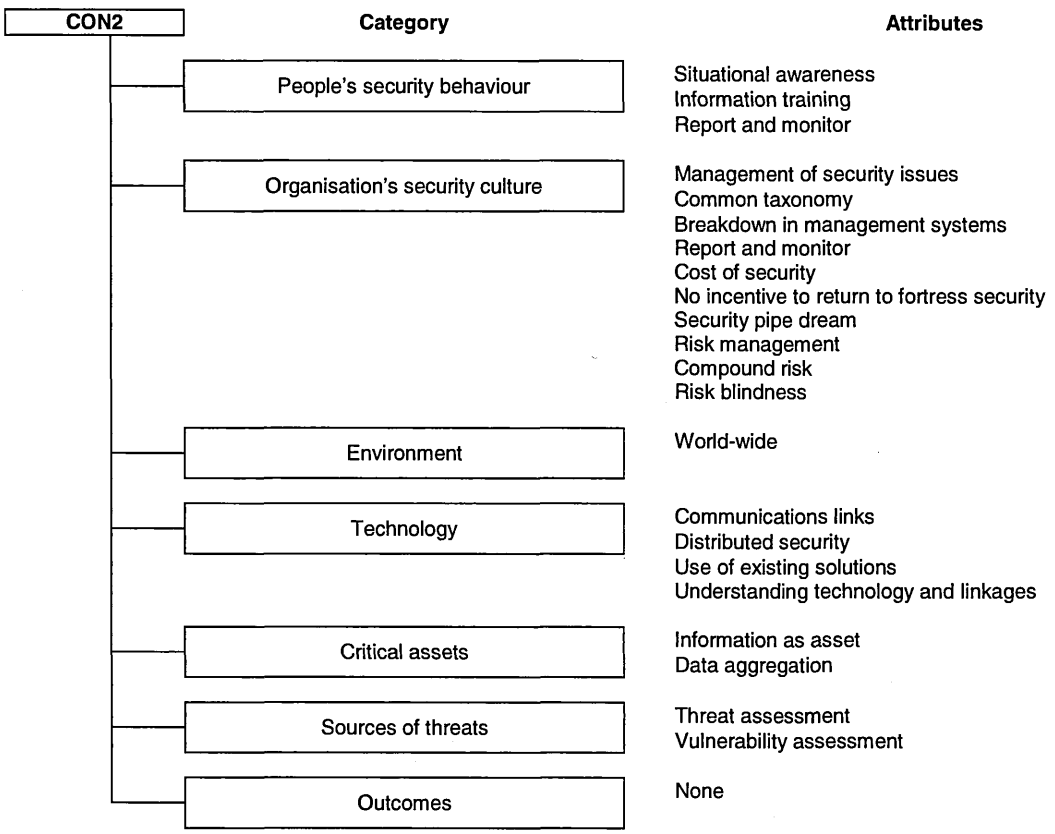


CON2 2nd September 2009

Author's note: This interview was conducted as an informal discussion of security principles because the interviewee has no sea going experience.

Data block and question	Interviewee's opinions of ICT security in a maritime environment	Researcher's interpretation of interviewee's opinions	Research code
A	The challenges faced in delivering situational awareness.	1. Delivering situational awareness	541. Situational awareness
B	The difficulty defending your own and others information.	1. Defending information	542. Information as asset
C	Difficulties maintaining communication links.	1. Maintaining communications links	543. Communications links
D	It is difficult to bring security principles to bear at extreme distances.	1. Distributed security	544. World-wide 545. Distributed security
E	What do I need to do, what do I need to prosecute, how do I prosecute it and how can I do that keeping a high quality of IA to do it? So what technical solutions are available for me to do that?	1. Plan 2. Develop 3. Implement 4. Look to technical solutions that are tried and tested	546. Management 547. Existing solutions
F	A common [MODUK] understanding of terminology remains a challenge. Indeed, the use of [MODUK] terminology is different from that used in government.	1. The need for a common taxonomy	548. Common taxonomy
G	There is a lack of understanding of how information can be used correctly and that training is required to overcome this. The lack of understanding of the technology makes it difficult to understand security risks. When you lose the understanding of the integral linkages between security, management information, knowledge management and exploit information starts to break down.	1. Information as asset not understood 2. Training required to overcome lack of understanding 3. Lack of understanding of the technology and linkages makes it difficult to plan for security 4. Information management starts to break down	549. Information a asset 550. Information training 551. Understanding technology and linkages 552. Breakdown in management systems
H	MODUK losses of information are starting to drop off.	1. Rates of incidents falling in 2009	553. Report and monitor
I	There is no money to go back to an entirely risk free world – and life isn't risk free.	1. No money to return to fortress security 2. Fortress security a bit of a myth anyway	554. Cost of security 555. No incentive to return to fortress security 556. Security pipe dream
J	Data aggregation and financial risk reaching 'critical' levels and a growing realisation that risk should not be allowed to stack up.	1. E.g. How many restricted documents in one place add up to secret? 2. Compound risk not a good thing	557. Data aggregation 558. Risk management 559. Compound risk
K	A good maritime threat and vulnerability analysis has not been conducted. As a result, decisions are being made without the full facts.	1. Needs threat and vulnerability assessment 2. Decisions on security being made without the full facts	560. Threat assessment 561. Vulnerability assessment 562. Risk blind

CON2 Summary of initial analysis



CON3 2nd September 2009

Author's note: This interview was conducted as an informal discussion of security principles because the interviewee has no sea going experience.

Data block and question	Interviewee's opinions of ICT security in a maritime environment	Researcher's interpretation of interviewee's opinions	Research code
A	It is better to have security technology that supports people rather than technology with all the bells and whistles.	1. Security for the people.	563. Security by design
B	Bad security practice is a cause of incidents but also the need to get the job done leads to taking short cuts. If security practice is embedded in normal business then business practice should improve and management of risks become standard practice.	1. Peoples actions can cause security incidents. 2. Operational imperatives can override security practice. 3. Security should be part of normal business activity 4. Security risk management as standard practice.	564. People's behaviour 565. Security awareness 566. Operational imperatives 567. Security imperatives 568. Security by design 569. Security risk management
C	The new linkage between career progression and disciplinary action [The no blame culture is being replaced with facing the consequence of actions]. This is leading to improved behaviour.	1. Make people accountable for their actions. 2. Improved behaviour by threats of punitive response. 3. Replacing no blame culture.	570. Accountability 571. People's behaviour
D	Risk can be sensibly managed as long as mitigation processes are in place.	1. Risk management required 2. Contingency plans to mitigate against failure.	572. Risk management 573. Contingency
E	Raising consciousness (awareness), it identifies the frailties in explicit ways and helps to identify the investment strategy needed in order to improve. It would help if MODUK would adopt normal risk management processes in this area. However, MODUK is doing the right things; it just needs to get better. The security methodology and processes are good enough.	1. Awareness of the problems helps with vulnerability analysis and the best way to spend to improve security. 2. MODUK security could be better.	574. Security awareness 575. Vulnerability assessment 576. Operating costs 577. Security risk management
F	There is a need to apply the threat assessments and mitigation in the business context. There is also a need to embed security design into capability design so that it enables rather than dampens and weakens practice.	1. Security and operations must correspond. 2. Build security into the system from day one.	578. Threat assessment 579. Security by design
G	There is nothing worse than a bolted on security measure. The best way to achieve safety is by design from the first stage.	1. Bad security design can lead to lowering of morale. 2. Cost implications if security applied as an after-thought.	580. Security by design 581. People's behaviour 582. Security practices
H	An opportunity arose to chat about wider issues. He believes that ICT procurement across HMG should be based on design. Also talked about MODUK enterprise wide initiatives, one of which is the three part MODUK Information Strategy (MODIS).	1. ICT bought by HMG should have security by design. 2. MODUK initiatives must include security.	583. Security by design

CON3: Summary of initial analysis